2022 S.T. Yau High School Science Award (Asia)

Research Report

The Team

Registration Number: Math-112

Name of team member: KO Siu Ting

School: Pui Ching Middle School

Country: Hong Kong, China

Name of team member: WONG Yin Cheung

School: Pui Ching Middle School

Country: Hong Kong, China

Name of team member: YUNG Samantha

School: Pui Ching Middle School

Country: Hong Kong, China

Name of supervising teacher: FAN Yan Lam

Job Title: Mathematics Teacher

School: Pui Ching Middle School

Country: Hong Kong, China

Title of Research Report

Investigation on variables separating polynomials

Date

31 August 2022

Investigation on variables separating polynomials

KO Siu Ting, WONG Yin Cheung, YUNG Samantha

Abstract

In this paper, a polynomial $p(x, y)$ is said to be k**-separating** if $p(x, y)$ can be expressed as $a_1(x)b_1(y) + a_2(x)b_2(y) + \cdots + a_k(x)b_k(y)$. Our main questions are to determine the minimal number of k and find single-variable polynomials $a_i(x)$, $b_i(y)$ for given polynomial $p(x, y)$. We first prove that the minimal number k is the rank of the matrix of coefficients of $p(x, y)$. After that, we use Full Rank Factorization to find a decomposition of any $p(x, y)$. Furthermore, we generalise the problem to n variables over arbitrary fields. We provide upper and lower bounds of $\operatorname{rank} p$. In addition, we find a necessary and sufficient condition to determine the 1-separating polynomials in $\mathbb{F}_2[x, y, z]$. Finally, we study the special case where the degrees of x, y, z are at most 1. We then classify the polynomials p in this case according to their ranks.

Keywords: polynomial, matrix, rank, spanning set, dimension, full rank factorization, reduced row echelon form

Acknowledgement

We would like to thank Mr Bendit Tsz Hin Chan for the provision of his prestigious linear algebra notes and Mr Mark Tin Wai Lau for his advice. We would also like to thank Mr Healey Ho Fung Lee for the egg tart support and Ms On Ki Luo for the emotional support.

Commitment on Academic Honesty and Integrity

We hereby declare that we

1. are fully committed to the principle of honesty, integrity and fair play throughout the competition.
2. actually perform the research work ourselves and thus truly understand the content of the work.
3. observe the common standard of academic integrity adopted by most journals and degree theses.
4. have declared all the assistance and contribution we have received from any personnel, agency, institution, etc. for the research work.
5. undertake to avoid getting in touch with assessment panel members in a way that may lead to direct or indirect conflict of interest.
6. undertake to avoid any interaction with assessment panel members that would undermine the neutrality of the panel member and fairness of the assessment process.
7. observe all rules and regulations of the competition.
8. agree that the decision of YHSA(Asia) is final in all matters related to the competition.

We understand and agree that failure to honour the above commitments may lead to disqualification from the competition and/or removal of reward, if applicable; that any unethical deeds, if found, will be disclosed to the school principal of team member(s) and relevant parties if deemed necessary; and that the decision of YHSA(Asia) is final and no appeal will be accepted.

(Signatures of full team below)

X
Name of team member: KO Siu Ting

X
Name of team member: WONG Yin Cheung

X
Name of team member: YUNG Samantha

X
Name of supervising teacher: FAN Yan Lam

Noted and endorsed by

Name of school principal: HO Lik Ko, Pui Ching Middle School

Contents

1 Introduction

This investigation is inspired by a Putnam problem [1], which asks whether a given polynomial can be written as the sum of products of single-variable polynomials. The question and solution are presented below.

Question (Putnam 2003 B1, [1]). *Do there exist polynomials $a(x)$, $b(x)$, $c(y)$, $d(y)$ such that*

$$1 + xy + x^2y^2 = a(x)c(y) + b(x)d(y) \tag{1}$$

holds identically?

Answer ([1]). The answer to this question is false. Assume on a contrary that there is such a decomposition (1). Substitute $y = -1, 0, 1$ into (1), we have

$$\begin{aligned} 1 - x + x^2 &= a(x)c(-1) + b(x)d(-1), \\ 1 &= a(x)c(0) + b(x)d(0), \\ 1 + x + x^2 &= a(x)c(-1) + b(x)d(-1). \end{aligned}$$

Viewing the three polynomials as vectors in the vector space $\mathbb{R}[x]$, we conclude that the three linearly independent vectors are all linear combinations of $a(x)$ and $b(x)$. This leads to a contradiction.

Firstly, we generalise the Putnam problem in two aspects: (i) making the polynomial on the left-hand-side of (1) arbitrary and (ii) having different quantities of terms on the right-hand-side of (1).

Next, we see that linear algebra techniques are applied to solve the problem. It is expected that matrices methods are needed to solve a generalised problem. Mathematically, we introduce the following definition for our investigation.

Definition 1.1. *Let $p(x, y) \in \mathbb{R}[x, y]$ be a polynomial and let $k \in \mathbb{N}$. $p(x, y)$ is said to be **k-separating** if there exist polynomials $a_1(x), a_2(x), ..., a_k(x) \in \mathbb{R}[x]$ and $b_1(y), b_2(y), ..., b_k(y) \in \mathbb{R}[y]$ such that*

$$p(x, y) = a_1(x)b_1(y) + a_2(x)b_2(y) + \cdots + a_k(x)b_k(y).$$

*The zero polynomial is **0-separating** by convention. Moreover, we say $\operatorname{rank} p = k$ if p is k-separating, but not $(k-1)$-separating.*

Remark 1.2. In Section 3, we will investigate polynomials p in more than 2 variables over arbitrary fields.

The example below demonstrates the meaning of the above definition. It can be seen that the same polynomial is k-separating for different values of k, depending on how terms are arranged and factorised. The minimal value k is then of our major interest, since there are no trivial effective ways to determine it yet.

Example 1.3. Let $p(x,y) = x^4y^6 - 2x^4 + 2x^3y^6 - 4x^3 + y^6 - 2$. Write

$$p(x,y) = x^4 \cdot y^6 - 2x^4 \cdot 1 + 2x^3 \cdot y^6 - 4x^3 \cdot 1 + 1 \cdot y^6 - 2 \cdot 1.$$

Note that each term is expressed in the form $a(x)b(y)$, so $p(x,y)$ is 6-separating. Similarly, we observe that if the number of terms of $p(x,y)$ is N, then $p(x,y)$ is N-separating.

On the other hand, we can write

$$p(x,y) = x^4 \cdot (y^6 - 2) + x^3 \cdot (2y^6 - 4) + 1 \cdot (y^6 - 2).$$

Here, we group the terms with the same degree of x, so $p(x,y)$ is 3-separating. Notice that we can also group the terms with the same degree of y and conclude that $p(x,y)$ is 2-separating:

$$p(x,y) = (x^4 + 2x^3 + 1) \cdot y^6 - (2x^4 + 4x^3 + 2) \cdot 1.$$

In this case, we observe that if the number of different powers of x and y in $p(x,y)$ are m and n respectively, then $p(x,y)$ is m-separating and n-separating. In fact, $p(x,y)$ can also be 1-separating (so $\operatorname{rank} p = 1$):

$$p(x,y) = (x^4 + 2x^3 + 1) \cdot (y^6 - 2).$$

From this example, various values of k are found so that $p(x,y)$ is k-separating, but it turns out that $\operatorname{rank} p = 1$ is a non-trivial fact. Naturally, we would like to obtain a systematic method to determine the rank of p and a decomposition of p. The main questions of this paper are stated below.

Question 1. *Given a polynomial* $p(x,y) \in \mathbb{R}[x,y]$, *determine* $\operatorname{rank} p$.

Question 2. *Given a polynomial* $p(x,y) \in \mathbb{R}[x,y]$ *with* $\operatorname{rank} p = k$, *find* $a_i(x) \in \mathbb{R}[x]$, $b_i(y) \in \mathbb{R}[y]$ *such that*

$$p(x,y) = a_1(x)b_1(y) + a_2(x)b_2(y) + \cdots + a_k(x)b_k(y).$$

In section 2, solutions to the two main questions are presented. The solutions involve the usage of matrices. In Section 3, we further generalised the above settings to polynomials with more than two variables over arbitrary fields, in which complexity grows exponentially. In particular, we investigate the special case of low-degree polynomials in $\mathbb{F}_2[x,y,z]$.

2 Separating polynomials in 2 variables

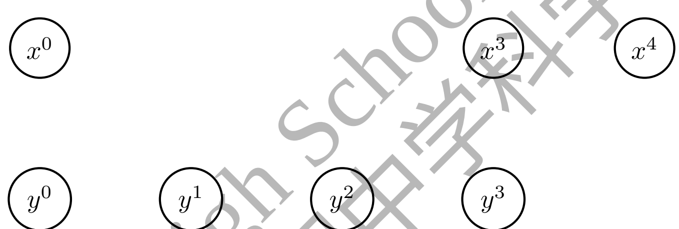
2.1 1-separating

We begin our investigation with the simplest case – to determine whether a given polynomial $p(x, y)$ is 1-separating, that is,

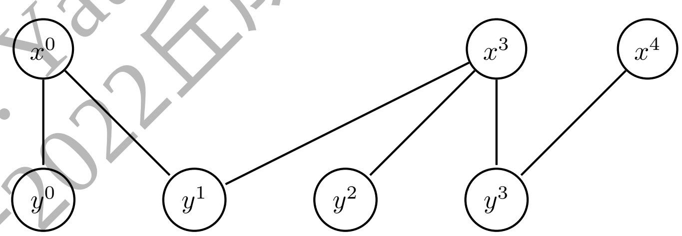
$$p(x,y) = a(x)b(y), \quad a(x) \in \mathbb{R}[x], \quad b(y) \in \mathbb{R}[y].$$

In this case, we notice that the powers of x and y in $p(x, y)$ must appear in $a(x)$ and $b(y)$ respectively. Referring to the polynomial $p(x, y)$ in Example 1.3, $a(x)$ must contain the terms x^0, x^3 and x^4, while $b(y)$ must contain the terms y^0 and y^6. Then, by expanding $a(x)b(y)$, all cross-terms x^0y^0, x^0y^6, x^3y^0, x^3y^6, x^4y^0 and x^4y^6 must exist. As a first approach, we use a graph to represent a given polynomial and then determine whether it is 1-separating. An example is given below.

Example 2.1. Let $p(x, y) = 7 + 3y + 2x^3y + 9x^3y^2 + x^3y^3 + 4x^4y^3$. By listing out the powers of x and y in $p(x, y)$, we have the vertices:



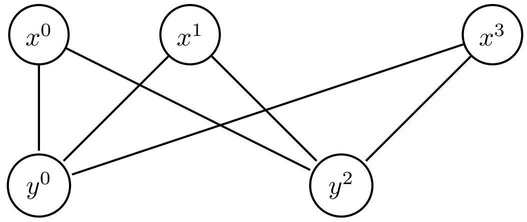
After that, the existing cross-terms in $p(x, y)$ are represented by edges connecting respective powers of x and y.



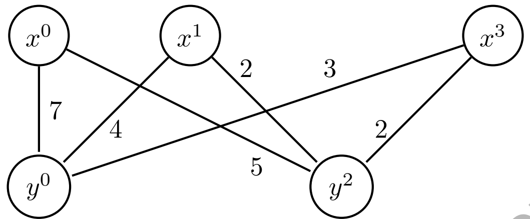
If the polynomial is 1-separating, all cross-terms must exist, which means that the graph should be a complete bipartite graph. From the graph above, some cross-terms are missing, so $p(x, y)$ is not 1-separating.

However, even if the graph is complete bipartite, $p(x, y)$ is not necessarily be 1-separating, as the coefficient of each term has to be considered too.

Example 2.2. Let $p(x, y) = 7 + 5y^2 + 4x + 2xy^2 + 3x^3 + 2x^3y^2$. Its graphical representation is:



Take the coefficients into consideration, we assign the coefficients to respective edges:



If $p(x,y) = a(x)b(y)$ is 1-separating, then

$$a(x) = \alpha_0 + \alpha_1 x + \alpha_3 x^3 \quad \text{and} \quad b(y) = \beta_0 + \beta_2 y^2 \quad \text{for some } \alpha_0, \alpha_1, \alpha_3, \beta_0, \beta_2 \in \mathbb{R}.$$

Notice that the coefficient of $x^i y^j$ is equal to $\alpha_i \beta_j$. Without loss of generality, take $\alpha_3 = 1$ and we have $\beta_2 = 2$ and $\beta_0 = 3$. By looking at the coefficients of $x^0 y^2$ and $x^0 y^0$, we have $2\alpha_0 = 5$ and $3\alpha_0 = 7$, which yields a contradiction. Thus $p(x,y)$ is not 1-separating.

Clearly, the problem is more complicated when we have to consider the coefficients in the graph. Also, this method is limited to 1-separating polynomials only. Instead, let us introduce a clearer and more systematic representation of a polynomial, as follows.

Definition 2.3. *Let $p(x,y) \in \mathbb{R}[x,y]$ be a polynomial. Define **the matrix associated to** $p(x,y)$ to be*

$$P = \begin{pmatrix} p_{00} & p_{01} & \cdots & p_{0n} \\ p_{10} & p_{11} & \cdots & p_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{m0} & p_{m1} & \cdots & p_{mn} \end{pmatrix},$$

where p_{ij} denotes the coefficient of $x^i y^j$ in $p(x,y)$.

Remark 2.4. The indices of the entries start from 0 so as to match the indices of the polynomial. Also, m and n are the maximum degrees of x and y in p respectively.

Definition 2.5. *Let P be a matrix and $\vec{p}_i$ be its rows, where $1 \le i \le m$. Define the **row space** of P to be*

$$\mathrm{RSp}(P) = \mathrm{Span}\{\vec{p}_1, \vec{p}_2, ..., \vec{p}_m\}.$$

We first focus on the simplest case, which is 1-separating. Here, we would like to find out how to determine whether a polynomial is 1-separating. Given a 1-separating polynomial $p(x,y) = (1+x)(1+y)$, it can also be written as $1 \cdot (1+y) + x \cdot (1+y)$. As $1 \cdot (1+y)$ and $x \cdot (1+y)$ are all multiples of $1+y$, the two rows in P are linearly dependent and the rank of P is 1. As a result, we have the following theorem.

Theorem 2.6. *Let $p(x,y) \in \mathbb{R}[x,y]$ and P be the matrix associated to $p(x,y)$. Then $p(x,y)$ is 1-separating if and only if* $\operatorname{rank} P \leq 1$.

Proof. ($\Rightarrow$) Let $p(x,y) = a(x)b(y)$ for some $a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ and $b(y) = \beta_0 + \beta_1 y + \cdots + \beta_n y^n$. Then we have $p_{ij} = \alpha_i \beta_j$, i.e.

$$\begin{pmatrix} p_{00} & \dots & p_{0n} \\ \vdots & \ddots & \vdots \\ p_{m0} & \dots & p_{mn} \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 & \cdots & \alpha_0\beta_n \\ \vdots & \ddots & \vdots \\ \alpha_m\beta_0 & \dots & \alpha_m\beta_n \end{pmatrix}.$$

Since each row is a multiple of $(\beta_0, \beta_1, \cdots, \beta_n)$, we have $\operatorname{rank} P \leq 1$.

($\Leftarrow$) If $\operatorname{rank} P \leq 1$, then $\operatorname{RSp}(P) = \operatorname{Span}(\vec{v})$ for some row vector $\vec{v} = (\beta_0, \beta_1, \cdots, \beta_n)$ and so the i^{th} row of P is $\alpha_i \vec{v}$ for some $\alpha_i \in \mathbb{R}$. We have

$$P = \begin{pmatrix} \alpha_0\vec{v} \\ \vdots \\ \alpha_m\vec{v} \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 & \cdots & \alpha_0\beta_n \\ \vdots & \ddots & \vdots \\ \alpha_m\beta_0 & \cdots & \alpha_m\beta_n \end{pmatrix}.$$

By picking $a(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_m x^m$ and $b(y) = \beta_0 + \beta_1 y + \cdots + \beta_n y^n$, we have $p(x,y) = a(x)b(y)$, which is 1-separating. □

2.2 k-separating

In the previous subsection, we have found a way to identify rank-1 polynomials. In this subsection, we continue to determine the rank of any given polynomial.

If $p(x,y) = p_1(x,y) + p_2(x,y)$, where $p_1(x,y)$ and $p_2(x,y)$ are both 1-separating, then $p(x,y)$ can be written in the form $a(x)b(y) + c(x)d(y)$ and so it is 2-separating. Hence, we decompose $p(x,y)$ into a sum of 1-separating polynomials. The following lemma is needed before presenting the main theorem.

Lemma 2.7. *For any matrices A and B,* $\operatorname{rank}(A+B) \leq \operatorname{rank} A + \operatorname{rank} B$.

Proof. Let $\vec{a}_i$ and $\vec{b}_i$ be the rows of A and B respectively. Further let $s = \operatorname{rank} A$, $t = \operatorname{rank} B$, and $\{\vec{a}'_1, \dots, \vec{a}'_s\}$ and $\{\vec{b}'_1, \dots, \vec{b}'_t\}$ be bases for $\operatorname{RSp}(A)$ and $\operatorname{RSp}(B)$ respectively. For any $\vec{v} \in \operatorname{RSp}(A+B)$, there exist

$\gamma_1, \ldots, \gamma_n \in \mathbb{R}$ such that

$$\begin{aligned} v &= \gamma_1(\vec{a}_1 + \vec{b}_1) + \cdots + \gamma_n(\vec{a}_n + \vec{b}_n) \\ &= (\gamma_1\vec{a}_1 + \cdots + \gamma_n\vec{a}_n) + (\gamma_1\vec{b}_1 + \cdots + \gamma_n\vec{b}_n). \end{aligned}$$

Since $\gamma_1\vec{a}_1 + \cdots + \gamma_n\vec{a}_n \in \mathrm{RSp}(A)$ and $\gamma_1\vec{b}_1 + \cdots + \gamma_n\vec{b}_n \in \mathrm{RSp}(B)$, we have

$$\begin{aligned} \gamma_1\vec{a}_1 + \cdots + \gamma_n\vec{a}_n &= \mu_1\vec{a}'_1 + \cdots + \mu_s\vec{a}'_s \quad \text{for some } \mu_1, ..., \mu_s \in \mathbb{R}, \\ \gamma_1\vec{b}_1 + \cdots + \gamma_n\vec{b}_n &= \lambda_1\vec{b}'_1 + \cdots + \lambda_t\vec{b}'_t \quad \text{for some } \lambda_1, ..., \lambda_t \in \mathbb{R}. \end{aligned}$$

Therefore, $v = (\mu_1\vec{a}'_1 + \cdots + \mu_s\vec{a}'_s) + (\lambda_1\vec{b}'_1 + \cdots + \lambda_t\vec{b}'_t) \in \mathrm{Span}\{a_1, \cdots, a_s, b_1, \cdots, b_t\}$, so $\mathrm{rank}(A+B) \leq s + t = \mathrm{rank}\, A + \mathrm{rank}\, B$. □

The following is the main theorem of this section, which generalises the idea in Theorem 2.6.

Theorem 2.8. *Let $p(x,y) \in \mathbb{R}[x,y]$ and P be the matrix associated to $p(x,y)$. Then $p(x,y)$ is k-separating if and only if* $\mathrm{rank}\, P \leq k$.

Proof. ($\Rightarrow$) Suppose $p(x,y)$ is k-separating. Let $p(x,y) = a_1(x)b_1(y) + a_2(x)b_2(y) + \cdots + a_k(x)b_k(y)$. Let $p_i = a_i(x)b_i(y)$ for $i = 1, \ldots, k$, i.e. $p(x,y) = p_1 + p_2 + \cdots + p_k$. Let P_i be the matrix associated to p_i (with the same dimension as P). By Lemma 2.7 and Theorem 2.6,

$$\begin{aligned} \mathrm{rank}\, P &= \mathrm{rank}(P_1 + \cdots + P_k) \\ &\leq \mathrm{rank}\, P_1 + \cdots + \mathrm{rank}\, P_k \\ &\leq 1 + \cdots + 1 \\ &\leq k. \end{aligned}$$

($\Leftarrow$) Let $\vec{p}_0 \ldots, \vec{p}_m$ be the rows of P. As $\mathrm{rank}\, P \leq k$, we can let $\mathrm{RSp}(P) = \mathrm{Span}\{\vec{p}'_1, \ldots, \vec{p}'_k\}$. For each $\vec{p}_i \in \mathrm{RSp}(P)$, there exist $\gamma_{ij} \in \mathbb{R}$ such that $\vec{p}_i = \sum \gamma_{ij}\vec{p}'_j$. As a result,

$$P = \begin{pmatrix} \vec{p}_0 \\ \vec{p}_1 \\ \vdots \\ \vec{p}_m \end{pmatrix} = \begin{pmatrix} \gamma_{01}\vec{p}'_1 \\ \gamma_{11}\vec{p}'_1 \\ \vdots \\ \gamma_{m1}\vec{p}'_1 \end{pmatrix} + \begin{pmatrix} \gamma_{02}\vec{p}'_2 \\ \gamma_{12}\vec{p}'_2 \\ \vdots \\ \gamma_{m2}\vec{p}'_2 \end{pmatrix} + \cdots + \begin{pmatrix} \gamma_{0k}\vec{p}'_k \\ \gamma_{1k}\vec{p}'_k \\ \vdots \\ \gamma_{mk}\vec{p}'_k \end{pmatrix}.$$

Write $\vec{p}'_i = (\beta_{i0}, \beta_{i1}, ..., \beta_{in})$. Take $a_i(x) = \gamma_{0i} + \gamma_{1i}x + \cdots + \gamma_{mi}x^m$ and $b_i(y) = \beta_{i0} + \beta_{i1}y + \cdots + \beta_{in}y^n$. Then

$$p(x,y) = a_1(x)b_1(y) + \cdots + a_k(x)b_k(y).$$

As a result, $p(x, y)$ is k-separating. $\square$

As a corollary, the rank of a polynomial is equal to the rank of the matrix associated to it. This also justifies the terminology of the rank of a polynomial in Definition 1.1.

Corollary 2.9. *Let $p(x, y) \in \mathbb{R}[x, y]$ and P be the matrix associated to $p(x, y)$. Then* $\operatorname{rank} p = \operatorname{rank} P$.

Proof. Let $\operatorname{rank} p = k$. Then p is k-separating but not $k-1$-separating. By Theorem 2.8, we have $\operatorname{rank} P \leq k$ and $\operatorname{rank} P > k - 1$. Hence, $\operatorname{rank} P = k$. $\square$

2.3 Computing decomposition

In the previous subsection, we have determined the rank of any given polynomial, which answered Question 1. In this section, we would like to solve Question 2, that is, to compute decomposition of any given polynomial.

The key observation is that the matrix representation of a 1-separating polynomial $a(x)b(y)$ can be factorized into a product of a column vector and a row vector. For example, if $p(x, y) = (x^2 + 2x + 1)(y^2 - 2)$, then the matrix associated to p is

$$P = \begin{pmatrix} 1 & 0 & -2 \\ 2 & 0 & -4 \\ 1 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \end{pmatrix}.$$

Base on this observation, we use the Full Rank Factorization method ([3]) to compute a decomposition of any given polynomial. The theorem is stated without proof here.

Theorem 2.10 (Full Rank Factorization, [3])**.** *Let P be a matrix with* $\operatorname{rank} P = r$. *Then $P = CR$, where C is composed by the first r independent columns of P and R contains the r nonzero rows of the reduced row echelon form of P.*

We illustrate the computation with an example below.

Example 2.11. Let $p(x, y) = 3x^2y^2 + 5x^2y + x^2 + 3xy^2 + 7xy + 2x + y^2 + 3y + 1$. Then the matrix associated to p is

$$P = \begin{pmatrix} 1 & 3 & 1 \\ 2 & 7 & 3 \\ 1 & 5 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} = B,$$

where B is in reduced echelon form. Note that $\operatorname{rank} P = 2$. Then C is obtained by removing the third column of P, and R is obtained by removing the third row of B, so

$$C = \begin{pmatrix} 1 & 3 \\ 2 & 7 \\ 1 & 5 \end{pmatrix}, R = \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \end{pmatrix}.$$

Then

$$P = CR = \begin{pmatrix} 1 & 3 \\ 2 & 7 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -2 \end{pmatrix} + \begin{pmatrix} 3 \\ 7 \\ 5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}.$$

As a result, we can write $p(x,y) = (1+2x+x^2)(1-2y^2) + (3+7x+5x^2)(y+y^2)$, which is 2-separating.

Notice that the resulting decomposition is found in ascending degree of y. Thus, we would ask whether there are any ways to find a decomposition with specific constraints. In particular, we will use the same $p(x,y)$ in Example 2.11 to illustrate how to compute the decomposition in descending degree of x.

Example 2.12. First we list the coefficient p_{ij} in reversed order. The corresponding matrix is given below.

$$P = \begin{pmatrix} 3 & 3 & 1 \\ 5 & 7 & 3 \\ 1 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -1/3 \\ 0 & 1 & 2/3 \\ 0 & 0 & 0 \end{pmatrix} = B,$$

where B is in reduced echelon form and rank $P = 2$. Then C is obtained by removing the third column of P, and R is obtained by removing the third row of B, so

$$C = \begin{pmatrix} 3 & 3 \\ 5 & 7 \\ 1 & 2 \end{pmatrix}, R = \begin{pmatrix} 1 & 0 & -1/3 \\ 0 & 1 & 2/3 \end{pmatrix}.$$

Then

$$P = CR = \begin{pmatrix} 3 & 3 \\ 5 & 7 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1/3 \\ 0 & 1 & 2/3 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1/3 \end{pmatrix} + \begin{pmatrix} 3 \\ 7 \\ 2 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2/3 \end{pmatrix}.$$

As a result, we can write $p(x,y) = (x^2 - 1/3)(3y^2+5y+1) + (x+2/3)(3y^2+7y+2)$, which is in descending power of x.

While we are investigating different cases, we discover that the expression of a k-separating polynomial may not be unique. For example, let $p(x,y) = x^2y + xy + x + y + 1$. Then

$$p(x,y) = x^2y + (x+1)(y+1) = (x^2+x+1)y + (x+1)\cdot 1$$

admits two different 2-separating expressions. This also shows an example that the expression of separations of $p(x,y)$ in the decreasing degree of x is not unique.

Since arranging the degree of x in descending order is not enough to decompose $p(x,y)$ uniquely, we would like to see if the expression $p(x,y)$ can be unique if we fix both the degrees of x and y in descending order. However, this is not possible for all $p(x,y)$:

Example 2.13. Let $p(x,y) = x^4y + xy^5$. From Corollary 2.9, $\operatorname{rank} p = 2$. Assume $p(x,y) = a_1(x)b_1(y) + a_2(x)b_2(y)$, where $\deg a_1 > \deg a_2$ and $\deg b_1 > \deg b_2$. Then $\deg a_1 = 4$ and $\deg b_1 = 5$, which produce the term x^4y^5. However, since $\deg a_2 < 4$ and $\deg b_2 < 5$, it is impossible for the term x^4y^5 to be cancelled. Since $p(x,y)$ does not contain the term x^4y^5, this is a contradiction, i.e. $p(x,y)$ cannot be expressed with degree of x and y being strictly decreasing.

3 Separating polynomials in more than 2 variables

After we completely solved the two questions in the previous section, a natural generalisation is to investigate polynomials with more than two variables over arbitrary fields. We restate Definition 1.1 in this setting.

Definition 3.1 (c.f. Definition 1.1)**.** *Let K be a field, $n,k \in \mathbb{N}$, and $p(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ be a polynomial. $p(x_1,\ldots,x_n)$ is said to be k-**separating** if there exist polynomials $a_{ij}(x_j) \in K[x_j]$ for $1 \le i \le k$ and $1 \le j \le n$ such that*

$$p(x_1,\ldots,x_n) = \sum_{i=1}^{k} a_{i1}(x_1)a_{i2}(x_2)\cdots a_{in}(x_n).$$

*The zero polynomial is **0-separating** by convention. Moreover, we say $\operatorname{rank} p = k$ if p is k-separating, but not $(k-1)$-separating.*

We introduce some of the notations in this section for better readability. In this section, a recurring step is to decompose the polynomial according to the power of one of the variables.

Definition 3.2. *Given a polynomial $p(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$,*

- *the x_n**-decomposition** of p is*

$$p(x_1,\ldots,x_n) = \sum_{i=0}^{N} q_i(x_1,\ldots,x_{n-1})\cdot x_n^i,$$

where N is the maximum degree of x_n in p. Note that this decomposition of p exists and is unique.

- *the x_n**-set** Q (of p) is the set $\{q_0,\ldots,q_N\} \subseteq K[x_1,\ldots,x_{n-1}]$.*

Definition 3.3. *Let V be a subspace of $K[x_1, \dots, x_n]$, for some $n \in \mathbb{N}$. We define $\dim_1 V$ to be the minimum number of rank-1 polynomials needed to span V.*

The following theorem relates the rank of a polynomial to the definitions above:

Theorem 3.4. *Let Q be the x_n-set of p. Then $\operatorname{rank} p = \dim_1 \operatorname{Span} Q$.*

Proof. $(\leq)$. Let $\dim_1 \operatorname{Span} Q = d$. So $\operatorname{Span} Q$ can be spanned by some $\alpha_1, \dots, \alpha_d \in K[x_1, \dots, x_{n-1}]$, all of which are rank-1. Suppose the x_n-decomposition of p is

$$p(x_1, \dots, x_n) = \sum_{i=0}^{N} q_i(x_1, \dots, x_{n-1}) \cdot x_n^i.$$

By definition, $Q = \{q_0, \dots, q_N\}$, and in particular $q_0, \dots, q_N \in \operatorname{Span} Q$. Hence,

$$q_i = \sum_{j=1}^{d} \lambda_{ij} \alpha_j$$

for some $\lambda_{ij} \in K$. Now

$$p = \sum_{i=0}^{N} \sum_{j=1}^{d} \lambda_{ij} \alpha_j \cdot x_n^i = \sum_{j=1}^{d} \left(\alpha_j \sum_{i=0}^{N} \lambda_{ij} \cdot x_n^i \right),$$

which is a sum of d polynomials with rank-1. Therefore, p is d-separating, thus $\operatorname{rank} p \leq d$.

$(\geq)$. Let $\operatorname{rank} p = r$, so there exists polynomials $a_{ij}(x_j) \in K[x_j]$ for $1 \leq i \leq r$ and $1 \leq j \leq n$ such that

$$p = \sum_{i=1}^{r} a_{i1}(x_1) \cdots a_{in}(x_n).$$

Now write $a_{in}(x_n) = \sum_{j=0}^{N} \lambda_{ij} x_n^j$ for $N \in \mathbb{N}$ and some $\lambda_{ij} \in K$. Then

$$\begin{aligned} p &= \sum_{i=1}^{r} a_{i1}(x_1) \cdots a_{i(n-1)}(x_{n-1}) \cdot \sum_{j=0}^{N} \lambda_{ij} x_n^j \\ &= \sum_{j=0}^{N} \sum_{i=1}^{r} \lambda_{ij} a_{i1}(x_1) \cdots a_{i(n-1)}(x_{n-1}) \cdot x_n^j. \end{aligned} \tag{$*$}$$

By comparing the coefficients of x_n^j of $(*)$ and the x_n-decomposition of p, we have

$$q_j = \sum_{i=1}^{r} \lambda_{ij} a_{i1}(x_1) \cdots a_{i(n-1)}(x_{n-1}) \quad \forall j.$$

Hence, $\{a_{i1}(x_1) \cdots a_{i(n-1)}(x_{n-1}) : 1 \leq i \leq r\}$ is a set containing rank-1 polynomials which spans $\operatorname{Span} Q$, so $r \geq \dim_1 \operatorname{Span} Q$. ∎

Using Theorem 3.4, we obtain a lower bound and an upper bound of $\operatorname{rank} p$:

Theorem 3.5. *Let $p(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ be a polynomial with x_n-set Q. Then*

$$\dim \operatorname{Span} Q \leq \operatorname{rank} p \leq \sum_{q \in Q} \operatorname{rank} q.$$

Proof. (Lower bound). Let $\operatorname{rank} p = r$. By Theorem 3.4, $r = \dim_1 \operatorname{Span} Q$, so there exists r polynomials $\alpha_1, \dots, \alpha_r$ which spans $\operatorname{Span} Q$, all of which are rank 1. In particular, $\operatorname{Span} Q = \operatorname{Span}\{\alpha_1, \dots, \alpha_r\}$ so $\dim \operatorname{Span} Q \leq r$, as needed.

(Upper bound). As in the proof of Theorem 3.4, we write $p = \sum q_i x_n^i$ and thus $Q = \{q_0, \dots, q_N\}$. Set $\operatorname{rank} q_i = k_i$, then we can write

$$p = \sum_{i=0}^{N} \sum_{j=1}^{k_i} r_{ij} \cdot x_n^i$$

for rank 1 polynomials $r_{ij} \in K[x_1, \dots, x_{n-1}]$, for $1 \leq j \leq k_i$. This is a sum of $\sum_{q \in Q} \operatorname{rank} q = k_0 + \cdots + k_N$ polynomials, so p is $\left(\sum_{q \in Q} \operatorname{rank} q\right)$-separating. By Definition 3.1, $\operatorname{rank} p \leq \sum_{q \in Q} \operatorname{rank} q$. □

Remark 3.6. In general, the first inequality may not be an equality. Here is an example: Consider

$$\begin{aligned} p(x, y, z) &= x^2 + xyz + 2z \\ &= (xy + 2)z + (x^2). \end{aligned}$$

Hence, $Q = \{xy + 2, x^2\}$ and so $\dim \operatorname{Span} Q \leq 2$. However, one can check that $\dim_1 \operatorname{Span} Q = 3$.

We then discovered that if we consider $K[x, y]$ as $K[x] \otimes K[y]$, determining the rank of polynomials is equivalent to determining the rank of their corresponding tensors, that is

$$\sum_{i=1}^{n} a_i(x) \times b_i(y) \longleftrightarrow \sum_{i=1}^{n} a_i(x) \otimes b_i(y).$$

In the case of more than 2 variables, determining the rank of tensors is NP-hard [4] for a general field K. Thus, we restrict the problem to $K = \mathbb{F}_2$ to see if any conclusions can be made.

3.1 Separating polynomials in $\mathbb{F}_2[x, y, z]$

We first consider polynomials in $\mathbb{F}_2[x, y, z]$ with 1-separating.

Notation. *Let $p(x, y, z) \in \mathbb{F}_2[x, y, z]$. Denote p_{ijk} as the coefficient of $x^i y^j z^k$ in p, and define*

$$\begin{aligned} I &= \{i \in \mathbb{N} : p_{ijk} = 1 \text{ for some } j, k\}, \\ J &= \{j \in \mathbb{N} : p_{ijk} = 1 \text{ for some } i, k\}, \\ K &= \{k \in \mathbb{N} : p_{ijk} = 1 \text{ for some } i, j\}, \\ S &= \{(i, j, k) \in \mathbb{N}^3 : p_{ijk} = 1\}. \end{aligned}$$

Lemma 3.7. *$S \subseteq I \times J \times K$.*

Proof. Pick $(i, j, k) \in S$. By the definition of S, $p_{ijk} = 1$ and from the definition of I, J, K, $i \in I, j \in J, k \in K$, thus $(i, j, k) \in I \times J \times K$ and $S \subseteq I \times J \times K$. $\square$

Theorem 3.8. *p is 1-separating if and only if $|S| = |I| \cdot |J| \cdot |K|$. In this case,*

$$p = \left(\sum_{i\in I} x^i\right)\left(\sum_{j\in J} y^j\right)\left(\sum_{k\in K} z^k\right).$$

Proof. ($\Rightarrow$) Since p is 1-separating, let $p = a(x)b(y)c(z)$, where $a = \sum \alpha_i x^i$, $b = \sum \beta_j y^j$, $c = \sum \gamma_k z^k$. Then $p_{ijk} = \alpha_i \beta_j \gamma_k$.

Pick any $i_0 \in I, j_0 \in J, k_0 \in K$, we have $(i_0, j_0, k_0) \in I \times J \times K$. Since $i_0 \in I$, there exists some j' and k' such that $p_{i_0 j' k'} = 1$. Thus, p is non-zero and there exists at least a j', k' such that $\beta_{j'} = \gamma_{k'} = 1$. In this case, we have $\alpha_{i_0} = 1$. Similarly, $\alpha_{i_0} = \beta_{j_0} = \gamma_{k_0} = 1$, then we have

$$p_{i_0 j_0 k_0} = \alpha_{i_0}\beta_{j_0}\gamma_{k_0} = 1,$$

which indicates that $(i_0, j_0, k_0) \in S$ and $I \times J \times K \subseteq S$.

From Lemma 3.7, $S \subseteq I \times J \times K$, so we have $S = I \times J \times K$ and $|S| = |I \times J \times K| = |I||J||K|$.

($\Leftarrow$) From Lemma 3.7, $S \subseteq I \times J \times K$. Suppose $S \neq I \times J \times K$, then $|I| \cdot |J| \cdot |K| = |I \times J \times K| > |S|$, which contradicts to $|S| = |I| \cdot |J| \cdot |K|$. It then remains to show that p is 1-separating given that $S = I \times J \times K$. But

$$\begin{aligned}\left(\sum_{i\in I} x^i\right)\left(\sum_{j\in J} y^j\right)\left(\sum_{k\in K} z^k\right) &= \sum_{(i,j,k)\in I\times J\times K} x^i y^j z^k \\ &= \sum_{(i,j,k)\in S} x^i y^j z^k \\ &= p.\end{aligned}$$

$\square$

Although we present the proof of Theorem 3.8 in $\mathbb{F}_2[x, y, z]$, the idea can be extended to $\mathbb{F}_2[x_1, \ldots, x_n]$. We omit the details here due to cumbersome notations.

3.2 Low-degree polynomials in $\mathbb{F}_2[x, y, z]$

In this subsection, we consider polynomials in three variables **with degrees of x, y, z at most** 1. We fix the following notations in our discussion. Let

$$p(x, y, z) = q_0(x, y) + q_1(x, y)z$$

be the z-decomposition of p. We shall denote by Q_0 and Q_1 the matrix associated to q_0 and q_1 respectively. We also define S_0, S_1, S_2 to be the set of 2×2 rank-0, rank-1 and rank-2 matrices in $\mathbb{F}_2$, i.e.

$$\begin{aligned}
S_0 &= \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}, \\
S_1 &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \right\}, \\
S_2 &= \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.
\end{aligned}$$

Lemma 3.9. *Let a, b, c be non-negative integers. Suppose any polynomial $p(x, y, z)$ with z-decomposition $q_0 + q_1 z$ where $(\operatorname{rank} q_0, \operatorname{rank} q_1, \operatorname{rank}(q_0 + q_1)) = (a, b, c)$ has $\operatorname{rank} k$. Then*

$$\operatorname{rank}(q_0' + q_1' z) = k$$

for any polynomials $q_0'(x, y), q_1'(x, y)$ with degree of x and y at most 1 such that $(\operatorname{rank} q_0', \operatorname{rank} q_1', \operatorname{rank}(q_0' + q_1'))$ is a permutation of (a, b, c), i.e.

$$(\operatorname{rank} q_0', \operatorname{rank} q_1', \operatorname{rank}(q_0' + q_1')) \in \{(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)\}.$$

Proof. Let q_0', q_1' be polynomials such that $\sigma := (\operatorname{rank} q_0', \operatorname{rank} q_1', \operatorname{rank}(q_0' + q_1'))$ is a permutation of (a, b, c). Define two polynomials q_0, q_1 based on σ:

$$(q_0, q_1) = \begin{cases} (q_0', q_1') & \sigma = (a, b, c), \\ (q_0', q_0' + q_1') & \sigma = (a, c, b), \\ (q_1', q_0') & \sigma = (b, a, c), \\ (q_1', q_0' + q_1') & \sigma = (b, c, a), \\ (q_0' + q_1', q_0') & \sigma = (c, a, b), \\ (q_0' + q_1', q_1') & \sigma = (c, b, a). \end{cases}$$

Note that in any case, $\operatorname{Span}\{q_0', q_1'\} = \operatorname{Span}\{q_0, q_1\}$. But $p = q_0 + q_1 z$ satisfies the given condition; namely, we have $(\operatorname{rank} q_0, \operatorname{rank} q_1, \operatorname{rank}(q_0 + q_1)) = (a, b, c)$. Hence $\operatorname{rank} p = k$, and by Theorem 3.4,

$$\operatorname{rank}(q_0' + q_1' z) = \dim_1 \operatorname{Span}\{q_0', q_1'\} = \dim_1 \operatorname{Span}\{q_0, q_1\} = \operatorname{rank} p = k.$$

$\square$

Remark 3.10. Lemma 3.9 tells us that $\operatorname{rank}(q_0 + q_1 z)$ is invariant under permutation of the condition on $(\operatorname{rank} q_0, \operatorname{rank} q_1, \operatorname{rank}(q_0+q_1))$. For instance, if we proved $\operatorname{rank}(q_0+q_1z)=1$ for all q_0, q_1 satisfying $(\operatorname{rank} q_0, \operatorname{rank} q_1, \operatorname{rank}(q_0+q_1)) = (1,1,0)$, then $\operatorname{rank}(q_0'+q_1'z)=1$ for all q_0', q_1' satisfying

$$(\operatorname{rank} q_0', \operatorname{rank} q_1', \operatorname{rank}(q_0'+q_1')) = (1,0,1) \text{ or } (0,1,1).$$

Moreover, notice that if $\operatorname{rank} p = k$, then the polynomial is k-separating and not $(k-1)$-separating. Hence, the two conditions are also invariant under the mentioned permutation.

Lemma 3.11. *$p(x,y,z)$ is rank-1 if and only if one of the following conditions is satisfied:*

(i) $Q_1 \in S_1$, $Q_0 = 0$.

(ii) $Q_1 = 0$, $Q_0 \in S_1$.

(iii) $Q_1 = Q_0 \in S_1$.

Proof. ($\Rightarrow$) Since $p(x,y,z)$ is 1-separating, we set $p(x,y,z) = a(x)b(y)c(z)$. Note that the only possible choices of $c(z)$ are $1, z$ and $z+1$. Hence, when

- $c(z) = z$: we have $p = 0 \cdot 1 + a(x)b(y)\cdot z$, so $Q_0 = 0$ and $Q_1 \in S_1$.
- $c(z) = 1$: similarly, $Q_0 \in S_1$ and $Q_1 = 0$.
- $c(z) = z+1$: we have $p = a(x)b(y)\cdot 1 + a(x)b(y)\cdot z$, so $Q_0 = Q_1 \in S_1$.

($\Leftarrow$) For (i), we have $p = q_1(x,y)\cdot z$. Since $\operatorname{rank} q_1 = 1$, $\operatorname{rank} p = 1$. The same conclusion holds for (ii) similarly. For (iii), we have

$$p = q_1(x,y)\cdot z + q_0(x,y) = q_0(x,y)\cdot(z+1).$$

Hence $\operatorname{rank} p = 1$. □

Theorem 3.12. *Let $p(x,y,z) \in \mathbb{F}_2[x,y,z]$. Define*

$$f = \operatorname{rank} Q_0 + \operatorname{rank} Q_1 + \operatorname{rank}(Q_0+Q_1).$$

(i) If $f = 0$, then $\operatorname{rank} p = 0$.

(ii) If $f = 2$, then $\operatorname{rank} p = 1$.

(iii) If $f = 3$ or 4, then $\operatorname{rank} p = 2$.

(iv) If $f = 5$ or 6 , then $\operatorname{rank} p = 3$.

Remark 3.13. Notice that $f = 1$ is impossible. If $f = 1$, we have the following cases:

	rank Q_0	rank Q_1	rank$(Q_0 + Q_1)$
I	0	0	1
II	0	1	0
III	1	0	0

Notice that the sum of any two of the matrices $Q_0, Q_1, Q_0 + Q_1$ equals to the remaining one. In all cases, two of $Q_0, Q_1, Q_0 + Q_1$ is 0, which forces the remaining matrix to be 0. This contradicts to its rank being 1.

Proof. (i) If $f = 0$, then $Q_0 = Q_1 = 0$. Hence $p(x, y, z) = 0$ so $\operatorname{rank} p = 0$.

(ii) If $f = 2$, we have the following cases:

	rank Q_0	rank Q_1	rank$(Q_0 + Q_1)$
I	2	0	0
II	0	2	0
III	0	0	2
IV	1	1	0
V	1	0	1
VI	0	1	1

- Case I to III are impossible, with the same explanation as in the remark above.
- Case IV to VI correspond to the three cases in Lemma 3.11, so $\operatorname{rank} p = 1$.

(iii) If $f = 3$, we have the following cases:

	rank Q_0	rank Q_1	rank$(Q_0 + Q_1)$
I	0	1	2
II	0	2	1
III	1	0	2
IV	2	0	1
V	1	2	0
VI	2	1	0
VII	1	1	1

- Case I to VI are impossible. When one of $Q_0, Q_1, Q_0 + Q_1$ is 0, it will force the other two matrices to be equal (of the same rank), which yields a contradiction.
- For case VII, notice that $\operatorname{rank} q_0 = \operatorname{rank} q_0 = 1$, so

$$p(x, y, z) = q_1(x, y) \cdot z + q_0(x, y) \cdot 1$$

is 2-separating. On the other hand, assuming $p(x,y,z)$ is 1-separating, then $Q_0 = Q_1$ and hence $\operatorname{rank}(Q_0+Q_1)=0$, which yields a contradiction. It follows that $\operatorname{rank} p = 2$.

(iv) If $f=4$, we have the following cases:

	$\operatorname{rank} Q_0$	$\operatorname{rank} Q_1$	$\operatorname{rank}(Q_0+Q_1)$
I	2	2	0
II	2	0	2
III	0	2	2
IV	1	1	2
V	1	2	1
VI	2	1	1

- In all cases, $p(x,y,z)$ is not 1-separating because Q_0 and Q_1 do not satisfy any condition in Lemma 3.11.
- In case I, $Q_0 = Q_1 \in S_2$, so $q_0 = q_1$ are 2-separating. Hence

$$p(x,y,z) = q_1(x,y)z + q_0(x,y) = q_0(x,y)(z+1)$$

  is also 2-separating. Thus, we have $\operatorname{rank} p = 2$. By Lemma 3.9, $\operatorname{rank} p$ is also 2 in case II and III.
- In case IV, $p(x,y,z)$ is 2-separating by the same argument as in (iii), Case VII. Thus, we have $\operatorname{rank} p = 2$. By Lemma 3.9, It follows that $\operatorname{rank} p = 2$ in case V and VI.

(v) If $f=5$, we have the following cases:

	$\operatorname{rank} Q_0$	$\operatorname{rank} Q_1$	$\operatorname{rank}(Q_0+Q_1)$
I	1	2	2
II	2	1	2
III	2	2	1

- In case I, we can write p as a sum of a 2-separating polynomial and a 1-separating polynomial so any polynomial in case I, II, III is 3-separating by Lemma 3.9.
- In case III, assume p is 2-separating. Then $\dim_1 \operatorname{Span}\{Q_0, Q_1\} = \operatorname{rank} p \le 2$, so there exists rank-1 matrices A, B and $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{F}_2$ such that

$$Q_0 = \alpha_0 A + \beta_0 B \quad \text{and} \quad Q_1 = \alpha_1 A + \beta_1 B.$$

  Since $Q_0, Q_1 \in S_2$, $Q_0 = Q_1 = A+B$. But then $Q_0+Q_1 = 0$, which yields a contradiction. Again, by Lemma 3.9, any polynomial in case I, II, III is not 2-separating.

(vi) If $f = 6$, we have the following cases:

$\operatorname{rank} Q_0$	$\operatorname{rank} Q_1$	$\operatorname{rank}(Q_0 + Q_1)$
2	2	2

Similar to case III above, p is not 2-separating. Now, we partition S_2 into two disjoint set.

$$S_2' = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \quad S_2'' = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

By calculations, the only possible choice for Q_0 and Q_1 is that $Q_0 \neq Q_1 \in S_2'$ or $Q_0 \neq Q_1 \in S_2''$. Also, any matrix in S_2' is a linear combination of the rank-1 matrices

$$\left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right\};$$

while any matrix in S_2'' is a linear combination of the rank-1 matrices

$$\left\{ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \right\}.$$

If $Q_0, Q_1 \in S_2'$, then

$$Q_0 = \alpha_1 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \alpha_2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \alpha_3 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad Q_1 = \beta_1 \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \beta_2 \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \beta_3 \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

for some $\alpha_i, \beta_i \in \mathbb{F}_2$. Thus, we see that p is 3-separating:

$$\begin{aligned} p &= (\alpha_1 + \beta_1 z)(xy + x + y + 1) + (\alpha_2 + \beta_2 z)(1) + (\alpha_3 + \beta_3 z)(xy) \\ &= (\alpha_1 + \beta_1 z)(x + 1)(y + 1) + (\alpha_2 + \beta_2 z)(1) + (\alpha_3 + \beta_3 z)(xy). \end{aligned}$$

Similarly, the same result holds if $Q_0, Q_1 \in S_2''$. The result follows. □

4 Conclusion

In this paper, we have investigated k-separating polynomials in two variables and generalised them into n variables. For the case of two variables, we proved that $\operatorname{rank} p$ is equal to the rank of the matrix P associated to the polynomial $p(x, y)$. We also used Full Rank Factorization ([3]) to provide a decomposition of $p(x, y)$.

However, the cases of polynomials with more than two variables become more complex. Indeed, we found out that this problem is equivalent to the well-known tensor rank problem, which is proved to be NP-hard

([4]). Although we cannot find a general formula to determine rank p, partial results were established. For example, we found upper and lower bounds of rank p, and proved a necessary and sufficient condition for a polynomial in $\mathbb{F}_2[x, y, z]$ to be 1-separating,

At last, we studied polynomials in $\mathbb{F}_2[x, y, z]$ with degrees of x, y, z at most 1 in great detail. In particular, we classified the polynomials p by $\operatorname{rank} Q_0 + \operatorname{rank} Q_1 + \operatorname{rank}(Q_0 + Q_1)$ in this case according to their ranks.

References

[1] L. F. Klosinski, G. L. Alexanderson & L. C. Larson (2004), *The Sixty-Fourth William Lowell Putnam Mathematical Competition*, The American Mathematical Monthly, 111:8, 680-690, DOI: 10.1080/00029890.2004.11920129.

[2] S. H. Friedberg and A. J. Insel and L. E. Spence (2002), Linear Algebra (4th Ed.), Pearson

[3] R. Piziak, P. L. Odell (1999), *Full Rank Factorization of Matrices*, Mathematics Magazine, Vol. 72(3), p.193-201

[4] Y. Shitov (2016), *How Hard Is The Tensor Rank?*, ArXiv, `https://arxiv.org/abs/1611.01559`

[5] B. Chan (2022) *Linear Algebra*, Online resources, `https://benditchan.files.wordpress.com/2022/03/lin_alg.pdf`