SEMI-REGULARITY OF PAIRS OF BOOLEAN POLYNOMIALS

TIMOTHY J. HODGES AND HARI R. IYER

ABSTRACT. Semi-regular sequences over $\mathbb{F}_2$ are sequences of homogeneous elements of the algebra $B^{(n)} = \mathbb{F}_2[X_1, ..., X_n]/(X_1^2, ..., X_n^2)$, which have a given Hilbert series and can be thought of as having as few relations between them as possible. It is believed that most such systems are semi-regular and this property has important consequences for understanding the complexity of Gröbner basis algorithms such as F4 and F5 for solving such systems. We investigate the case where the sequence has length two and give an almost complete description of the number of semi-regular sequences for each n.

1. INTRODUCTION

The concept of $\mathbb{F}_2$-*semi-regularity* was introduced in [1, 2] in order to assess the complexity of certain Gröbner basis algorithms applied to solving systems of equations over the Galois field $\mathbb{F}_2$. For $\mathbb{F}_2$-semi-regular systems one can determine explicitly the highest degree of polynomials that will arise in the application of these Gröbner basis algorithms and this information enables one to predict with some accuracy the length of time taken by such an algorithm to solve a semi-regular system of equations in any given implementation. Systems of polynomial equations over $\mathbb{F}_2$ arise naturally in many diverse settings but in particular they have arisen recently in cryptography with respect to the analysis of the Hidden Field Equations cryptosystems and to the solution of the discrete logarithm problem.

Set $B = \mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2, \ldots, X_n^2)$. Let V be an m-dimensional subspace of the space B_2 of quadratic elements of B. The space V is semi-regular if the Hilbert series of the graded quotient ring B/BV is given by the polynomial

$$T_{n,m}(z) = \left[\frac{(1+z)^n}{(1+z^2)^m}\right]$$

where $[\sum_{i=0}^{\infty} a_i z^i]$ denotes the series $\sum_{i=0}^{\infty} a_i z^i$ truncated at the first i for which $a_i \leq 0$.

The question we would like to answer in general is: *What proportion of such spaces are semi-regular*? The total number of subspaces of dimension

Key words and phrases. Semi-regularity, finite field.

Corresponding author: Timothy Hodges, Department of Mathematical Sciences, University of Cincinnati, Cincinnati, OH 45221-0025, USA, email:timothy.hodges@uc.edu.

m is well-known - it is the cardinality of the Grassmanian $\mathrm{Gr}(m, B_2)$. Let

$$sr(n,m) = |\{V \in \mathrm{Gr}(m, B_2^n) \mid V \text{ is semi-regular}\}|$$

and let

$$p_{n,m} = \frac{sr(n,m)}{|\,\mathrm{Gr}(m, B_2^n)|}$$

It is conjectured that for m sufficiently large compared to n, this proportion tends to 1 as n tends to infinity. Very little is known about this conjecture. In particular, it is not even known whether there are infinitely many n for which $p(n,n) \neq 0$.It was shown in [8] that for any fixed m, we must have that $p_{n,m} = 0$ for sufficiently large n. The case when $m = 1$ is fairly easy and has been understood for a while. We give a brief review of this case in Section 4.

The purpose of this paper is to describe in detail the case when $m = 2$ and to give a fairly exact description of which 2-dimensional subspaces are semi-regular for all possible values of n. The hope is that by understanding the behavior in this situation we will gain insight on the more general problem. In Section 3 we show that no semi-regular two dimensional subspaces exist for $n \geq 9$; and in more generality that no semi-regular two dimensional subspaces exist for $n > 4m + 1$. In Section 5 we deal with the easy cases when $n = 3, 4, 5$ and 7. In the last two sections we consider the more complicated situations when $n = 6$ and 8.

This work complements recent work by Semaev and Tenti which describes the behavior in the overdetermined case when m is sufficiently large compared to n. In the case of a proper subspace $V \subset B_2$, of dimension $m > (n-1)(n-2)/6$, Theorem 1.1 of [10] gives a lower bound for the proportion of such spaces which are semi-regular and the authors show that this bound tends to 1 as n tends to infinity.

2. Background and Basics

Let $\mathbb{F} = \mathbb{F}_2$ be the field with two elements. Set

$$B = B^n = \mathbb{F}[X_1, \ldots, X_n]/(X_1^2, \ldots, X_n^2)$$

(we shall drop the superscript when there is no need to emphasize the number n); and let x_i denote the image of X_i in B. This ring inherits the structure of a strongly graded ring from the polynomial ring $\mathbb{F}[X_1, \ldots, X_n]$. That is, if we denote by B_k^n the span of the monomials $x_{1_1} \ldots x_{i_k}$ of degree k, then $B^n = \bigoplus_{k=0}^n B_k^n$ and $B_k^n B_m^n = B_{k+m}^n$. It is easy to see that $\dim B_k^n = \binom{n}{k}$ and that $\dim B^n = 2^n$. The monomials $x_{\mathbf{i}} = x_{1_1} \ldots x_{i_k}$ form a basis for B^n so an arbitrary element of B can be written as $b = \sum_{\mathbf{i}} a_{\mathbf{i}} x_{\mathbf{i}}$. We define the support of b to be

$$\mathrm{Supp}(b) = \{x_{\mathbf{i}} \mid a_{\mathbf{i}} \neq 0\}$$

In [2], the concept of a semi-regular sequence of elements of B was defined in the following iterative fashion.

Definition 2.1. Let $f_1, \dots, f_m \in B$ be a sequence of homogeneous polynomials with $\deg f_i = d_i$. Let

$$D_{f_1,\dots,f_m} = \min \left\{ k \mid \sum_{i=1}^{m} B_{k-d_i} f_i = B_k \right\}$$

The sequence $f_1, \dots, f_m \in B$ is *semi-regular* if for all $i = 1, 2, \dots, m$ and homogeneous $g \in B$

$$g f_i \in (f_1, \dots, f_{i-1}) \quad \text{and} \quad \deg(g) + \deg(f_i) < D_{n,m}$$

implies $g \in (f_1, \dots, f_i)$.

For any series $\sum_i a_i z^i$, we denote by $\left[\sum_i a_i z^i\right]$ the truncated series $\sum_i b_i z^i$ where $b_i = a_i$ if $a_j > 0$ for $j = 0, \dots, i$ and $b_i = 0$ otherwise.

Proposition 2.2. *Let $f_1, \dots, f_m \in B$ be a sequence of homogeneous polynomials with $\deg f_i = d_i$. The sequence $f_1, \dots, f_m$ is semi-regular if and only if the Hilbert series of the graded ring $B/(f_1, \dots, f_m)$ is given by*

$$HS_{B/(f_1,\dots,f_m)}(z) = \left[\frac{(1+z)^n}{\prod_{i=1}^{m}(1+z^{d_i})} \right]$$

This shows that the number $D_{f_1,\dots,f_m}$ is the same for any semi-regular sequence of degree $\mathbf{d}$. We call this number the *degree of regularity* of a semi-regular sequence of degree $\mathbf{d}$.

We are interested here in the case where all the f_i are quadratic (that is $d_i = 2$ for all i). In this case, Proposition 2.2 implies that if we restrict our attention to linearly independent sequences, then the semi-regularity of the sequence depends only on the subspace V of B_2 that they generate and not on the choice of f_i (note that if the sequence is linearly dependent, then it is never semi-regular so we may disregard this situation). For this reason, we find it more natural to discuss the semi-regularity of subspaces, rather than of sequences. Thus a quadratic subspace V of dimension m is semi-regular if

$$HS_{B/BV}(z) = \left[\frac{(1+z)^n}{(1+z^2)^m} \right]$$

Set

$$T_{m,n}(z) = \left[\frac{(1+z)^n}{(1+z^2)^m} \right], \text{ and } D_{n,m} = \deg \left[\frac{(1+z)^n}{(1+z^2)^m} \right] + 1$$

So $D_{n,m}$ is the degree of regularity of an m-dimensional semi-regular space of quadratic elements.

Another way of characterizing semi-regularity is that the only relation between the f_i's are the trivial ones in degrees less than $D_{n,m}$. Consider the linear maps $\phi_j \colon B_{j-2} \otimes V \to B_j$ given by $\phi_j(\sum_i b_i \otimes v_i) = \sum_i b_i v_i$. Let $R_j(V) = \ker \phi_j$. Inside $R_j(V)$ there is a subspace of "trivial relations" $T_j(V)$ spanned by the elements

(1) $b(v \otimes w - w \otimes v)$ where $v, w \in V$ and $b \in B_{j-4}$;
(2) $b(v \otimes v)$ where $v \in V$ and $b \in B_{j-4}$.

Theorem 2.3. [7, Theorem 3.8] *Let V be an m-dimensional subspace of B_2 and let $D = D_{n,m}$. Then V is semi-regular if and only if*

(1) $R_j(V) = T_j(V)$ *for all* $j < D$.
(2) $B_{D-2}V = B_D$

If $\{v_1, \dots, v_m\}$ is a basis for V, then it can be easily shown that

$$T_j(V) = \sum_{i \neq j} B_{j-4}(v_i \otimes v_j - v_j \otimes v_i) + \sum_i B_{j-4}(v_i \otimes v_i)$$

We are interesting in understanding the proportion of such spaces which are semi-regular. Note that the set of all m-dimensional subspaces is the Grassmannian $\mathrm{Gr}(m, B_2)$ and that the size of this set is well-known to be given by the formula

$$|\,\mathrm{Gr}(m, \mathbb{F}^t)| = \frac{(2^t-1)(2^t-2)\dots(2^t-2^{m-1})}{(2^m-1)(2^m-2)\dots(2^m-2^{m-1})}$$

Let

$$sr(n,m) = |\{V \in \mathrm{Gr}(m, B_2^n) \mid V \text{ is semi-regular}\}$$

and let

$$p_{n,m} = \frac{sr(n,m)}{|\,\mathrm{Gr}(m, B_2^n)|}$$

be the proportion of m-dimensional subspaces which are semi-regular. It is generally believed for m sufficiently large relative to n that $\lim_{n\to\infty} p_{n,m} = 0$. For instance, one can conjecture that for c sufficiently large,

$$\lim_{n\to\infty} p_{n,cn} = 1$$

We show here that for $c < 1/4$, this limit is 0.

The general linear group $\mathrm{GL}(B_1)$ acts naturally as graded automorphisms of the algebra B. It therefore acts as permutations of $\mathrm{Gr}(m, B_2^n)$. Thus we can decompose the Grassmannian as a union of $\mathrm{GL}(B_1)$-orbits and semi-regularity is an invariant of these orbits. Under the action of $\mathrm{GL}(B_1)$ every element of B_2 is equivalent to an element of the form $x_1x_2 + \dots + x_{m-1}x_m$. We call the number m the rank of b. There is an important connection between the rank and failure of semi-regularity due to the following result.

Theorem 2.4. [4, Corollary 2.2] *If $\mu \in B_2$ has rank k, then*

$$\dim \frac{\mathrm{Ann}(\mu) \cap B_d}{B_{d-2}\mu} = \binom{n-k}{d-k/2} 2^{k/2}$$

In particular, $\mathrm{Ann}(\mu) \cap B_d \supsetneq B_{d-2}\mu$ *when* $k/2 \leq d \leq n - k/2$.

This immediately yields the following condition on the ranks of elements of a semi-regular space.

Corollary 2.5. *If V is a semi-regular subspace of B_2^n, then V contains no elements of rank k if $k/2 + 2 < D_{n,m}$. In particular, in order for there to exist semi-regular subspaces of dimension m, we must have $D_{n,m} \leq n/2 + 2$.*

3. An Upper Bound on n

We begin by giving an explicit bound on n above which there are no m-dimensional semi-regular subspaces of B_2^n. This improves upon the result in [8, Theorem 5.1] which established that such a bound always existed. A version of this result which fully extends [8, Theorem 5.1] is given in the Appendix.

Lemma 3.1. *Given any $0 \neq a \in B$, there exists $b \in B$ such that $ab = x_1 \dots x_n$.*

Proof. Take a monomial m of smallest length in $\operatorname{Supp} a$. Say after renumbering, that $m = x_1 \dots x_k$. Then $m' = x_{k+1} \dots x_n$ must annihilate all the other elements of $\operatorname{Supp} a$. So $am' = mm' = x_1 \dots x_n$. □

Lemma 3.2. *If $t + j \leq n$, then $B_j \cap \operatorname{Ann} B_t = 0$. Equivalently, $\operatorname{Ann} B_t \cap \sum_{i=0}^{n-t} B_i = 0$.*

Proof. Let $a \in B_j \cap \operatorname{Ann} B_t$ where $j \leq n-t$. Then by the lemma there exists an element $b \in B_{n-j}$ such that $ab = x_1 \dots x_n$. But $b \in B_{n-j} = B_t B_{n-j-t}$, so

$$ab \in aB_{n-j} = aB_t B_{n-j-t} = 0$$

contradicting $ab \neq 0$. □

Theorem 3.3. *Let V be a subspace of B_2^n of dimension m and let $D = D_{n,m}$. If $n \geq D + 2m$, then $B_{D-2}V \neq B_D$; in particular V is not semi-regular.*

Proof. Let $B = \{\mu_1, \dots, \mu_m\}$ be a basis for V. Choose a subset $\{\mu_{i_1}, \dots, \mu_{i_s}\}$ which is maximal with respect to

$$\mu_{i_1} \dots \mu_{i_s} \neq 0$$

Then for any $i = 1, \dots, m$, $\mu_{i_1} \dots \mu_{i_s} \mu_i = 0$, so $\mu_{i_1} \dots \mu_{i_s} V = 0$. Suppose that $B_{D-2}V = B_D$. Then

$$\mu_{i_1} \cdot \dots \cdot \mu_{i_s} B_D = \mu_{i_1} \dots \mu_{i_s} B_{D-2} V = B_{D-2} \mu_{i_1} \dots \mu_{i_s} V = 0$$

This implies that $\mu_{i_1} \dots \mu_{i_s} \in B_{2s} \cap \operatorname{Ann} B_D = 0$. So Lemma 3.2 implies that $n < D + 2s \leq D + 2m$. Thus if $n \geq D + 2m$, then $B_{D-2}V \neq B_D$ and V is not semi-regular. □

Unfortunately the behavior of $D_{n,m}$ is too erratic for this result to give us an upper bound (for instance, even though $D_{n,m}$ grows slower than n for any fixed m, the difference $n - D_{n,m}$ is not an increasing function). This can be rectified somewhat using the following result.

Theorem 3.4. *There are no semi-regular m-dimensional subspaces of B_2^n when $n \geq 4(m+1)$*

Proof. Suppose that $n \geq 4(m+1)$; this implies that $n/2 + 2 \leq n - 2m$. Suppose that there exist semi-regular subspaces of dimension m. By Corollary 2.5, we must have that $D_{n,m} \leq n/2 + 2$. So $D_{n,m} \leq n - 2m$ contradicting Theorem 3.3. □

For small n one can always backfill the difference to get more exact answers.

Corollary 3.5. *There are no semi-regular subspaces of B_2^n:*

- *of dimension one for $n \geq 7$*
- *of dimension two for $n \geq 9$*
- *of dimension three for $n \geq 12$*
- *of dimension four for $n \geq 14$*

Proof. For instance when $m = 2$, Theorem 3.4 tells us that there are no semi-regular 2-dimensional subspaces for $n \geq 12$. For the cases $n = 9, 10, 11$, one can directly check that $D_{n,2} \leq n - 4$ so there are no 2-dimensional semi-regular subspaces in these cases. □

This leads to the following interesting conjecture:

Conjecture 3.6. For $m \neq 2$, there exist m-dimensional semi-regular subspaces of B_2^n if and only if $n \leq D_{n,m} + 2m$.

As we shall see, this conjecture is not true for $m = 2$. However, this would seem to be an exceptional case.

Theorem 3.4 also confirms the need for the condition on c in the Conjecture that $\lim_{n\to\infty} p_{n,cn} = 1$.

Corollary 3.7. *If $c < 1/4$, then $\lim_{n\to\infty} p_{n,cn} = 0$.*

Proof. If $c < 1/4$ then there exists an N such that for $n > N$, $cn \leq n/4 - 1$. So Theorem 3.4 implies that $p_{n,cn} = 0$ for $n > N$. □

4. The Case $m = 1$

Let us start by briefly reviewing the case when $m = 1$. In this case the Hilbert series and degree of regularity of a semi-regular space for small n are given by the following table

n	$T_{n,1}(z)$	$D_{n,1}$
3	$1 + 3z + 2z^2$	3
4	$1 + 4z + 5z^2$	3
5	$1 + 5z + 9z^2 + 5z^3$	4
6	$1 + 6z + 14z^2 + 14z^3 + z^4$	5
7	$1 + 7z + 20z^2 + 28z^3 + 15z^4$	5

Table 1. The Hilbert series and degree of regularity of a semi-regular 1-dimensional subspace

Lemma 4.1. *Suppose $n \geq 2$ and let $\mu \in B_2$. Then*

$$\dim B_1\mu = \begin{cases} n-2 & \text{if } \operatorname{rk}\mu = 2 \\ n & \text{if } \operatorname{rk}\mu \geq 4 \end{cases}$$

and

$$\dim B_2\mu = \begin{cases} \binom{n-2}{2} & \text{if } \operatorname{rk}\mu = 2 \\ \binom{n}{2} - 5 & \text{if } \operatorname{rk}\mu = 4 \\ \binom{n}{2} - 1 & \text{if } \operatorname{rk}\mu \geq 6 \end{cases}$$

Proof. Note that $\dim B_k\mu = \dim B_k - \dim \operatorname{Ann}(\mu) \cap B_k$. The result then follows directly from Theorem 2.4. □

Whether or not $V = \{0, \mu\}$ is semi-regular depends purely on the rank of μ.

Theorem 4.2. *Let $V = \{0, \mu\}$ be a one dimensional subspace of B_2.*

(1) When $n = 3$, all one dimensional spaces are semi-regular. So $p_{3,1} = 1$.
(2) When $n = 4$, V is semi-regular if and only if $\operatorname{rk}\mu = 4$. So $p_{4,1} = 28/63 \approx 0.44$.
(3) When $n = 5$, V is semi-regular if and only if $\operatorname{rk}\mu = 4$. So $p_{5,1} = 868/1023 \approx 0.85$
(4) When $n = 6$, V is semi-regular if and only if $\operatorname{rk}\mu = 6$. So $p_{6,1} = 13888/32767 \approx 0.42$
(5) When $n \geq 7$, no one dimensional spaces is semi-regular. Thus $p_{n,1} = 0$ for $n \geq 7$.

Proof. In the cases $n = 3, 4$, we have $D_{n,1} = 3$, so it suffices to verify the equality $B_1V = B_3$. Since $\dim B_3^3 = 1$ and $\dim B_3^4 = 4$, the result follows immediately from Lemma 4.1. In the case $n = 5$, we have $D_{5,1} = 4$, so we need to verify that the map $\phi_5 : B_1^5 \otimes V \to B_3^5$ is injective and the map $\phi_4 : B_2^5 \otimes V \to B_4^5$ is surjective. Lemma 4.1 implies that these conditions hold precisely when $\operatorname{rk}\mu = 4$. Finally, for $n = 6$, we need that $\dim B_1^6 V = 6$, $\dim B_2^6 V = 14$ and $B_3^6 V = B_5^3$. Lemma 4.1 implies that first two conditions hold only when $\operatorname{rk}\mu = 6$. The last condition is easily verified directly when $\operatorname{rk}\mu = 6$.

The figures for the proportions follow from the numbers of elements of each rank given in the following table

$r \backslash n$	3	4	5	6
2	7	35	155	651
4	0	28	868	18228
6	0	0	0	13888

TABLE 2. The number of elements of rank r in B_2^n

□

5. The Case $m = 2$ - Preliminaries

5.1. **Background and Notation.** We now consider two dimensional spaces. If $\dim V = 2$, then $V = \{0, \mu, \mu', \mu + \mu'\}$ for some $\mu.\mu' \in B_2^n$. An important invariant of this space is the triple

$$\mathrm{Rk}(V) = [\mathrm{rk}\,\mu, \mathrm{rk}\,\mu', \mathrm{rk}\,\mu + \mu'] \in \mathbb{N}^3/\Sigma_3$$

(that is, the equivalence class of the triple under the action of the symmetric group S_3). The number of spaces of the different rank types is given by a formula of Pott, Schmidt, and Zhou [9, Theorem 5]. Unfortunately the rank type of a space V does not determine its equivalence class under the action of $\mathrm{GL}(B_1)$. However it does provide an important and useful decomposition of the Grassmanian $\mathrm{Gr}(2, B_2)$.

5.2. **The cases $n = 3, 4, 5$ and 7.** From the table below we see that for $n = 3, 4,$ and 5 the degree of regularity is 3.

n	$T_{n,2}(z)$	$D_{n,2}$
3	$1 + 3z + z^2$	3
4	$1 + 4z + 4z^2$	3
5	$1 + 5z + 8z^2$	3
6	$1 + 6z + 13z^2 + 8z^3$	4
7	$1 + 7z + 19z^2 + 21z^3$	4
8	$1 + 8z + 26z^2 + 40z^3 + 17z^4$	5
9	$1 + 9z + 34z^2 + 66z^3 + 57z^4$	5

Table 3. The Hilbert series and degree of regularity of a semi-regular 2-dimensional subspace

Thus, in these cases, if V is a two dimensional subspace of B_2, then V is semi-regular if and only if the map $\phi_3 : B_1 \otimes V \to B_3$ is surjective; that is, if and only if $B_3 = B_1 V$.

Theorem 5.1. *If $n = 3$, then all two dimensional subspaces are semi-regular.*

Proof. In this case $\dim B_3 = 1$ and $B_1 V \neq 0$, so we must always have $B_3 = B_1 V$. □

Theorem 5.2. *Let $n = 4$ and let $V \subset B_2$ be a two dimensional subspace. Then V is semi-regular if and only if V contains an element of rank 4.*

Proof. Note that in this case $\dim B_3 = 4$. If $\operatorname{rk}\mu = 4$, then by Lemma 4.1, $\dim B_1\mu = 4$, so if V contains an element of rank 4, we must have $B_1V = B_3$. On the other hand, suppose that V is of type $[2,2,2]$ and let μ, μ' be a basis for V. Then $\mu = \lambda_1\lambda_2$ and $\mu' = \lambda_1'\lambda_2'$ for some $\lambda_1, \lambda_2, \lambda_1', \lambda_2' \in B_1$. Let $\Lambda = \operatorname{Span}(\lambda_1, \lambda_2, \lambda_1', \lambda_2')$. If $\dim \Lambda = 4$, then the λ's are linearly independent and $\mu + \mu'$ would have rank 4; on the other hand, if $\dim \Lambda = 2$, then $\dim \Lambda^2 = 1$ and $V \subset \Lambda^2$, a contradiction. Therefore we must have $\dim \Lambda = 3$. Hence we can find a subspace $V_0 \subset B_1$ such that $B_1 = \Lambda \oplus V_0$ and $\dim V_0 = 1$. But then

$$B_1V = \Lambda V + V_0V \subset \Lambda^3 + V_0V$$

Hence $\dim B_1V \leq \dim \Lambda^3 + \dim V_0V \leq 1 + 2 = 3$ and therefore $B_1V \neq B_3$. □

Corollary 5.3. *In the case $n = 4$, the proportion of subspaces of B_2^4 that are semi-regular is $p_{4,2} = 546/651 \approx 0.84$.*

Proof. The total number of two-dimensional subspaces is $|\operatorname{Gr}(m, B_2^4)| = 651$. From [9, Theorem 5], we have the number of subspaces of type $[2,2,2]$ is 105. So $p_{4,2} = (651 - 105)/651$. □

Now consider the case when $n = 5$. Note that $\dim B_3^5 = 10$ so $B_1V = B_3$ if and only if the map $\phi_3 : B_1^5 \otimes V \to B_3^5$ is an isomorphism.

Theorem 5.4. *The map $\phi_3 : B_1^5 \otimes V \to B_3^5$ is not surjective for any two dimensional subspace $V \subset B_2^5$. Hence there are no semi-regular two dimensional subspaces of B_2^5.*

Proof. We may assume, after appropriate change of variables, that $V = \{0, \mu, \mu', \mu + \mu'\}$ where $\mu \in B_2^4$ and $\mu' = \mu_0 + \lambda x_5$ for $\mu_0 \in B_2^4$ and $\lambda \in B_1^4$. Then

$$\begin{aligned} B_1V &= B_1\mu + B_1\mu' = (B_1^4 + \mathbb{F}x_5)\mu + (B_1^4 + \mathbb{F}x_5)(\mu_0 + \lambda x_5) \\ &= (B_1^4\mu + B_1^4\mu_0) + (\mathbb{F}\mu + \mathbb{F}\mu_0 + B_1^4\lambda)x_5 \end{aligned}$$

Now $B_3^5 = B_3^4 + B_2^4x_5$, so for this map to be surjective we must have $B_1^4\mu + B_1^4\mu_0 = B_3^4$ and $\mathbb{F}\mu + \mathbb{F}\mu_0 + B_1^4\lambda = B_2^4$. However $\dim B_1^4\lambda \leq 3$, so

$$\dim \mathbb{F}\mu + \mathbb{F}\mu' + B_1^4\lambda \leq 5 < 6 = \dim B_2^4$$

Thus $B_1V \neq B_3^5$ and V is not semi-regular. □

Next we jump ahead to consider the case when $n = 7$. Here the degree of regularity is four. So in order for the space V to be semi-regular we need the map $\phi_4 : B_2^7 \otimes V \to B_4^7$ to be surjective.

Theorem 5.5. *The map $\phi_4 : B_2^7 \otimes V \to B_4^7$ is not surjective for any 2-dimensional subspace $V \subset B_2^7$. Hence there are no semi-regular two dimensional subspaces of B_2^7.*

Proof. Pick a basis for V, say $\{\mu, \mu'\}$. After a suitable choice of generators we can assume that

$$\mu \in B_2^6, \quad \mu' = \mu_0 + \lambda x_7, \text{ where } \mu_0 \in B_2^6, \lambda \in B_1^6$$

Then

$$\begin{aligned} B_2^7 V &= B_2^7 \mu + B_2^7 \mu' \\ &= (B_2^6 + B_1^6 x_7)\mu + (B_2^6 + B_1^6 x_7)(\mu_0 + \lambda x_7) \\ &= (B_2^6 \mu + B_2^6 \mu_0) + (B_1^6 \mu + B_1^6 \mu_0 + B_2^6 \lambda) x_7 \end{aligned}$$

In order for ϕ_4 to be surjective we must have

$$B_1^6 \mu + B_1^6 \mu_0 + B_2^6 \lambda = B_3^6$$

If $\lambda = 0$, then we would have $B_1^6 \mu + B_1^6 \mu_0 = B_3^6$ which is impossible because the left hand side has dimension at most 12 and $\dim B_3^6 = 20$. So $\lambda \neq 0$. Consider the map $B^6 \to \tilde{B} = B^6/(\lambda) \cong B^5$. Denote the images of μ and μ_0 by $\tilde{\mu}$ and $\tilde{\mu}_0$. Then we would have

$$\tilde{B}_1 \tilde{\mu} + \tilde{B}_1 \tilde{\mu}_0 = \tilde{B}_3$$

But this contradicts Theorem 5.4. □

This yields an exact value for $p_{n,2}$ in all cases except $n = 6$ or 8. In the next two sections we consider these two remaining cases which are considerably more complicated.

6. The Case $m = 2$, $n = 6$

6.1. **Introduction.** Since $D_{6,2} = 4$, a two-dimensional space $V \subset B_2^6$ is semi-regular if

(1) the map $\phi_3 : B_1^6 \otimes V \to B_3^6$ is injective; and
(2) the map $\phi_4 : B_2^6 \otimes V \to B_4^6$ is surjective

Note that $\dim B_1^6 = 6$, $\dim B_2^6 = 15$, $\dim B_3^6 = 20$, and $\dim B_4^6 = 15$.

Proposition 6.1. *If V contains an element of rank 2, then V is not semi-regular. In particular if V has rank type $[2,2,2], [2,2,4], [2,4,4]$ or $[2,4,6]$, then V is not semi-regular.*

Proof. Corollary 2.5. □

This leaves the cases where V has rank type $[4,4,4], [4,4,6], [4,6,6]$ and $[6,6,6]$. In the case where V contains an element of rank 6 the surjectivity condition is easily established.

Lemma 6.2. *If V contains an element of rank 6, then the map $\phi_4 : B_2^6 \otimes V \to B_4^6$ is surjective.*

Proof. We may assume that the element of rank 6 is $\mu = x_1x_2+x_3x_4+x_5x_6$. Then $B_2^6\mu$ contains all the monomials of B_4^6 except

$$x_1x_2x_3x_4, x_1x_2x_5x_6, x_3x_4x_5x_6$$

In addition it contains

$$(x_1x_2 + x_3x_4)x_5x_6, (x_1x_2 + x_5x_6)x_3x_4, (x_3x_4 + x_5x_6)x_1x_2$$

Let μ' be another non-zero element of V. Suppose that we have a monomial $x_ix_j \in \mathrm{Supp}(\mu')$ which is not one of x_1x_2, x_3x_4, x_5x_6. Without loss of generality suppose it is x_1x_3. Then $x_1x_2x_3x_4 \in \mathrm{Supp}(x_2x_4\mu')$. Since $B_2^6\mu$ contains all the other monomials involving x_2x_4, B_2^6V must contain $x_1x_2x_3x_4$ and so $B_2^6V = B_4^6$. Now suppose that $\mathrm{Supp}(\mu') \subset \{x_1x_2, x_3x_4, x_5x_6\}$ and $\mu' \neq \mu$ so μ' is the sum of one or two of these terms. It is easily verified that in this case again $B_2^6V = B_4^6$. □

Lemma 6.3. *Suppose that $n \geq 6$ and let V be a 2-dimensional subspace of B_2^n. If V contains an element of rank at least 6, then $\mathrm{Ann}\, V \cap B_2^n = 0$. If, in addition, V has no elements of rank 2, then the map $\phi_3 : B_1^n \otimes V \to B_3^n$ is injective.*

Proof. Suppose that $V = \langle \mu, \mu' \rangle$ where $\mathrm{rk}\, \mu \geq 6$ and $\mu' \neq \mu$. Since $\mathrm{rk}\, \mu \geq 6$, we know from Lemma 4.1 that $\mathrm{Ann}\, \mu \cap B_2 = \{0, \mu\}$. Therefore $\mu'\mu \neq 0$ and $\mu \notin \mathrm{Ann}\, \mu' \cap B_2$. Hence

$$\begin{aligned}\mathrm{Ann}\, V \cap B_2 &= (\mathrm{Ann}\, \mu \cap B_2) \cap (\mathrm{Ann}\, \mu' \cap B_2)\\ &= \{0, \mu\} \cap (\mathrm{Ann}\, \mu' \cap B_2) = \{0\}\end{aligned}$$

Now assume that $\mathrm{rk}\, \mu'$ and $\mathrm{rk}(\mu + \mu')$ are both at least 4. An element of $\mathrm{Ker}\, \phi_3$ is of the form $a \otimes \mu + b \otimes \mu'$ where $a, b \in B_1$ and

$$a\mu + b\mu' = 0$$

But then $ab\mu = 0$ and $ab\mu' = 0$ so $ab \in \mathrm{Ann}\, V \cap B_2 = \{0\}$. Hence $a \in \mathrm{Ann}\, b \cap B_1 = \{0, b\}$. If $a = 0$, then $b\mu' = 0$, so $b = 0$ since $\mathrm{rk}\, \mu' \geq 4$. If $a = b$ then $a(\mu + \mu') = 0$, so $a = b = 0$ since $\mathrm{rk}(\mu + \mu') \geq 4$. Thus $\mathrm{Ker}\, \phi_3 = 0$. □

Theorem 6.4. *If V is a a 2-dimensional subspace of B_2^6 of rank type* $[4, 4, 6], [4, 6, 6]$ *or* $[6, 6, 6]$ *then V is semi-regular.*

Proof. The injectivity condition follows from Lemma 6.3. The surjectivity condition follows from Lemma 6.2. □

6.2. **Spaces of rank type** $[4, 4, 4]$**.** If V contains a rank four element we can assume this element is of the form $\mu = x_1x_2 + x_3x_4$. Thus we may assume that $V = \langle \mu, \mu' \rangle = \{0, \mu, \mu', \mu + \mu'\}$ where

$$\begin{aligned}\mu &= x_1x_2 + x_3x_4\\ \mu' &= \mu_0 + \lambda_1x_5 + \lambda_2x_6 + \epsilon x_5x_6\end{aligned}$$

and $\mu_0 \in B_2^4$, $\lambda_1, \lambda_2 \in B_1^4$ and $\epsilon \in \{0, 1\}$.

Example 1. If $\epsilon = \mu_0 = 0, \lambda_1 = x_1, \lambda_2 = x_3$, we get

$$\begin{aligned} \mu &= x_1x_2 + x_3x_4 \\ \mu' &= x_1x_5 + x_3x_6 \\ \mu + \mu' &= x_1(x_2 + x_5) + x_3(x_4 + x_6) \end{aligned}$$

One can easily verify that in this case V is not semi-regular because B_2V does not contain $x_2x_4x_5x_6$. Note that in this example $V \subset \langle x_1, x_3\rangle B_1$.

Example 2. If $\mu_0 = x_1x_2, \lambda_1 = \lambda_2 = 0$, we get

$$\begin{aligned} \mu &= x_1x_2 + x_3x_4 \\ \mu' &= x_1x_2 + x_5x_6 \\ \mu + \mu' &= x_3x_4 + x_5x_6 \end{aligned}$$

One can verify directly in this case that V is semi-regular.

Lemma 6.5. *Let V be a two-dimensional subspace of rank type $[4, 4, 4]$. If either*

(1) V is induced (there is a proper subspace $W \subset B_1$ such that $V \subset W^2$); or

(2) there is a two-dimensional subspace $\Lambda \subset B_1$ such that $V \subset B_1\Lambda$,

then V is not semi-regular.

Proof. (1) Without loss of generality, we can assume that $V \subset B_2^5$. In this case,

$$B_2^6V = (B_2^5 + B_1^5x_6)V \subset B_2^5V + B_1^5Vx_6 \subset B_4^5 + B_1^5Vx_6$$

Since $B_4^6 = B_4^5 + B_3^5x_6$ and $B_1^5V \subsetneq B_3^5$ by Theorem 5.4, we cannot have $B_2^6V = B_4^6$.

(2) In this case, as in Example 1, $B_2V \subset B_3\Lambda \subsetneq B_4$ so V is not semi-regular. □

Theorem 6.6. *Let V be a two-dimensional subspace of rank type $[4, 4, 4]$. Then V is semi-regular if an only if it is equivalent to a space of the form given in Example 2*

Proof. Suppose that V is not of the sort described in Lemma 6.5. We may assume that V is generated by μ and μ' of the form

$$\begin{aligned} \mu &= x_1x_2 + x_3x_4 \\ \mu' &= \mu_0 + \lambda_1x_5 + \lambda_2x_6 + \epsilon x_5x_6 \end{aligned}$$

where $\mu, \mu_0 \in B_2^4$, $\lambda_1, \lambda_2 \in B_1^4$ and $\epsilon \in \{0, 1\}$. Let $\Lambda = \langle\lambda_1, \lambda_2\rangle$

First consider the case where $\epsilon = 0$. In this case we must have $\dim \Lambda = 2$, otherwise we would be in case (1) of Lemma 6.5. Extend $\{\lambda_1, \lambda_2\}$ to a basis $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ for B_1^4. Note that $B_2^4 = \lambda_1B_1^4 + \lambda_2B_1^4 + \mathbb{F}\lambda_3\lambda_4$. Therefore, since $V \not\subset \Lambda B_1$, we must have that either μ_0 or $\mu_0 + \mu$ is of the form

$\lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 \lambda_4$ for some $a_1, a_2 \in B_1^4$. Assuming without loss of generality that it is μ_0, we have that

$$\begin{aligned}\mu' &= \lambda_1 a_1 + \lambda_2 a_2 + \lambda_3 \lambda_4 + \lambda_1 x_5 + \lambda_2 x_6 \\ &= \lambda_1 (x_5 + a_1) + \lambda_2 (x_6 + a_2) + \lambda_3 \lambda_4\end{aligned}$$

which is of rank 6 because $\lambda_1, \lambda_2, \lambda_3, \lambda_4, (x_5 + a_1), (x_6 + a_2)$ form a basis for B_1^4. This contradicts the assumption that $\operatorname{rk} \mu' = 4$.

Thus we must have $\epsilon \neq 0$. In this case after an appropriate change of basis, we may assume that $\lambda_1 = \lambda_2 = 0$ and $\mu' = \mu_0 + x_5 x_6$. In this case $\operatorname{rk} \mu' = \operatorname{rk} \mu_0 + 2$, so $\operatorname{rk} \mu_0 = 2$; similarly $\operatorname{rk}(\mu + \mu_0) = 2$. Thus $\mu = \mu_0 + (\mu + \mu_0)$ and up to a linear change of variables we are in the case of Example 2. □

6.3. **The Number of Semi-Regular Subspaces.** The table below gives the numbers of subspaces of the different rank types using the results of [9, Theorem 5]

Type	Number
$[2, 2, 2]$	9,765
$[2, 2, 4]$	182,280
$[2, 4, 4]$	3,417,750
$[2, 4, 6]$	4,666,368
$[2, 6, 6]$	2,187,360
$[4, 4, 4]$	30,902,536
$[4, 4, 6]$	69,995,520
$[4, 6, 6]$	54,246,528
$[6, 6, 6]$	13,332,480
Total	178,940,587

TABLE 4. Decomposition of the Grassmanian $\operatorname{Gr}(2, B_2^6)$ by Rank Type

Theorem 6.7. *There are* $153,129,088$ *semi-regular 2-dimensional subspaces of* B_2^6*. Thus the proportion of such subspaces that are semi-regular is*

$$p_{6,2} = \frac{153,129,088}{178,940,587} \approx 86\%$$

Proof. From Proposition 6.1 and Theorem 6.4 it suffices to calculate the number of spaces of rank type $[4, 4, 4]$ that are semi-regular. By Theorem 6.6, such spaces are precisely the orbit of the space given in Example 2. The stabilizer of this space in $GL_6(\mathbb{F})$ is isomorphic to $(GL_2(\mathbb{F}) \times GL_2(\mathbb{F}) \times GL_2(\mathbb{F})) \rtimes \Sigma_3$ which has order 6^4. Hence the size of the orbit is

$$\frac{20,158,709,760}{1,296} = 15,554,560$$

Adding this number to the total number of subspaces of type $[4, 4, 6], [4, 6, 6]$ or $[6, 6, 6]$ given in the table, yields the claimed conclusion. □

7. The Case $n = 8$

In this case $D_{8,2} = 5$, so semi-regularity of a two-dimensional quadratic subspace V is equivalent to the following properties

- The map $\phi_3 : B_1 \otimes V \to B_3$ is injective
- The kernel of $\phi_4 : B_2 \otimes V \to B_4$ is the trivial kernel $T_4(V)$.
- The map $\phi_5 : B_3 \otimes V \to B_5$ is surjective.

Note that $\dim B_2 = 28$, $\dim B_3 = 56$, $\dim B_4 = 70$, and $\dim B_5 = 56$.

Throughout this section, unless stated otherwise, V will denote a two-dimensional subspace of B_2^8.

Lemma 7.1. *Let V be a semi-regular two-dimensional subspace of B_2^8 Then V contains no non-zero elements of rank less than or equal to 4.*

Proof. Corollary 2.5 □

Thus it remains to investigate semi-regularity when the rank of V is $[6,6,6], [6,6,8], [6,8,8]$ or $[8,8,8]$. Note that the injectivity of the map $\phi_3 : B_1 \otimes V \to B_3$ holds in all such cases by Lemma 6.3. We can easily eliminate the following special case.

Theorem 7.2. *Suppose that there exists a proper subspace $W \subset B_1$ such that $V \subset W^2$. Then the map $\phi_5 : B_3 \otimes V \to B_5$ is not surjective. Hence V is not semi-regular.*

Proof. Without loss of generality, we may assume $W = B_1^7$ and $V \subset W^2$. Now $B_3 = B_3^7 \oplus B_2^7 x_8$, so

$$B_3 V = B_3^7 V + B_2^7 V x_8$$

By Theorem 5.5, $B_2^7 V \subsetneq B_4^7$. Since $B_5 = B_5^7 \oplus B_4^7 x_8$ we must have $B_3 V \subsetneq B_5$ and the map is not surjective. □

In this situation (there exists a proper subspace $W \subset B_1$ such that $V \subset W^2$), we shall say that the space V is *induced from* W (or just *induced* if W is not specified).

Lemma 7.3. *Suppose that $V = \langle \mu, \mu' \rangle$. The map $\phi_4 : B_2 \otimes V \to B_4$ has trivial kernel if and only if $\operatorname{rk} \mu$ and $\operatorname{rk} \mu'$ are at least 6 and*

$$B_2 \mu \cap B_2 \mu' = \{0, \mu\mu'\}$$

Proof. The trivial kernel of the map $m : B_2 \otimes V \to B_4$ is three dimensional with basis $\{\mu \otimes \mu, \mu' \otimes \mu - \mu \otimes \mu', \mu' \otimes \mu'\}$. Thus the kernel is trivial if and only if $\dim B_2 V = \dim B_2 \otimes V - 3 = 53$.

If $\operatorname{rk} \mu \leq 4$, then by Lemma 4.1 the kernel of the map $B_2 \otimes \mathbb{F}\mu \to B_2\mu$ has dimension at least 5 and so $\ker m$ cannot be trivial. So suppose that μ and μ' both have rank at least 6. Then $\dim B_2\mu = \dim B_2\mu' = 27$ by Lemma 4.1. On the other hand $B_2 V = B_2\mu + B_2\mu'$ so the kernel is trivial if and only if $\dim B_2 V = 54 - \dim B_2\mu \cap B_2\mu' = 53$; that is, $\dim B_2\mu \cap B_2\mu' = 1$. Since $\mu\mu' \neq 0$ (by Lemma 4.1 again), this is equivalent to $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$. □

We now look in detail at the situation where V contains an element of rank 6.

Lemma 7.4. *Let $\mu = y_1y_2 + \cdots + y_{m-1}y_m$ be an element of rank m in B_2^n. Then the space $U(\mu) = \operatorname{Span}(y_1, \ldots, y_m)$ is independent of the choice of $y_1, \ldots y_m$.*

Proof. Suppose that

$$\mu = y_1y_2 + \cdots + y_{m-1}y_m = y_1'y_2' + \cdots + y_{m-1}'y_m'$$

for some $y_1, \ldots, y_m$ and $y_1', \ldots, y_m'$ in B_1. Since $\operatorname{rk}\mu = m$, the $y_1, \ldots, y_m$ and $y_1', \ldots, y_m'$ must be linearly independent; hence it suffices to show that $y_1, \ldots, y_m \in \operatorname{Span}(y_1', \ldots, y_m')$.

Without loss of generality, we can assume that $n = m + 1$. Extend $y_1', \ldots, y_m'$ to a basis $y_1', \ldots, y_m', y_n'$ for B_1^n. Write

$$y_i = \sum_{j=1}^{n} a_{ij} y_j'$$

for some $a_{ij} \in \mathbb{F}$. The coefficient of the monomial $y_j'y_n'$ in $y_1y_2+\cdots+y_{m-1}y_m$ is

$$0 = a_{1j}a_{2n} + a_{1n}a_{2j} + \cdots + a_{m-1,j}a_{mn} + a_{m-1,n}a_{mj}$$

If the conclusion is false there exists a k such that $y_k \notin \operatorname{Span}(y_1', \ldots, y_m')$; that is, $a_{kn} \neq 0$. After renumbering the y_i we may assume $k = 1$. Thus $a_{1n} = 1$ and

$$a_{2j} = a_{1j}a_{2n} + \sum_{k=2}^{m/2} (a_{2k-1,j}a_{2k,n} + a_{2k-1,n}a_{2k,j})$$

Hence

$$\begin{aligned}
y_2 &= \sum_{j=1}^{n} a_{2j} y_j' \\
&= \sum_{j=1}^{n} \left(a_{1j}a_{2n} + \sum_{k=2}^{m/2} (a_{2k-1,j}a_{2k,n} + a_{2k-1,n}a_{2k,j}) \right) y_j' \\
&= \sum_{j=1}^{n} a_{1j}a_{2n}y_j' + \sum_{k=2}^{m/2} \left(\sum_{j=1}^{n} a_{2k-1,j}a_{2k,n}y_j' + \sum_{j=1}^{n} a_{2k-1,n}a_{2k,j}y_j' \right) \\
&= a_{2n}y_1 + \sum_{k=2}^{m/2} a_{2k,n}y_{2k-1} + \sum_{k=2}^{m/2} a_{2k-1,n}y_{2k}
\end{aligned}$$

contradicting the linear independence of the y_i. Hence we must have all $y_1, \ldots, y_m \in \operatorname{Span}(y_1', \ldots, y_m')$, as required. □

Definition 7.5. Let V be a non-induced 2-dimensional subspace of B_2^8 containing an element μ of rank 6. We say that V is of

(A) Type A with respect to μ if $V \not\subset U(\mu)B_1$.
(B) Type B with respect to μ if $V \subset U(\mu)B_1$

Proposition 7.6. *Let V be a non-induced two dimensional subspace of B_2 containing an element μ of rank six.*

(1) If V is of Type A with respect to μ then there exists a basis $\{y_1, y_2, \ldots, y_8\}$ of B_1 such that $V = \mathrm{Span}(\mu, \mu')$ where $\mu = y_1y_2 + y_3y_4 + y_5y_6$ and $\mu' = \mu_0 + y_7y_8$ for some $\mu_0 \in B_2^6$.
(2) If V is of Type B with respect to μ then there exists a basis $\{y_1, y_2, \ldots, y_8\}$ of B_1 such that $V = \mathrm{Span}(\mu, \mu')$ where $\mu = y_1y_2 + y_3y_4 + y_5y_6$ and $\mu' = \mu_0 + \lambda y_7 + \lambda' y_8$ for some $\mu_0 \in B_2^6$ and some linearly independent $\lambda, \lambda' \in B_1^6$.

Proof. Since μ has rank six we may choose $y_1, \ldots, y_6$ such that $\mu = y_1y_2 + y_3y_4 + y_5y_6$ and the y_i are linearly independent. Extend $\{y_1, \ldots, y_6\}$ to a basis $\{y_1, \ldots, y_8\}$ for B_1. Pick $\mu' \in V \backslash \{0, \mu\}$. Then $\mu' = \mu_0 + \lambda y_7 + \lambda' y_8 + \eta y_7 y_8$ where $\mu_0 \in B_2^6$, $\lambda, \lambda' \in B_1^6$ and $\eta \in \mathbb{F}$. If $\eta = 1$, then

$$\mu' = (\mu_0 + \lambda\lambda') + (\lambda' + y_7)(\lambda + y_8)$$

So replacing y_7 with $\lambda' + y_7$ and y_8 with $\lambda' + y_8$ yields the required form. If $\eta = 0$ and $\dim\langle \lambda, \lambda' \rangle \leq 1$, then V is induced. So if V is non-induced and of type B we must have $\dim\langle \lambda, \lambda' \rangle = 2$. □

Notes that if V is a Type A space, V has rank type $[6, \mathrm{rk}(\mu_0) + 2, \mathrm{rk}(\mu + \mu_0) + 2]$.

Theorem 7.7. *Let V be a Type A subspace of rank type $[6, 6, 6]$, $[6, 6, 8]$ or $[6, 8, 8]$. Then V is semi-regular.*

Proof. By Proposition 7.6 we can assume that $V = \langle \mu, \mu' \rangle$ where

$$\mu = x_1x_2 + x_3x_4 + x_5x_6 \text{ and } \mu' = \mu_0 + x_7x_8$$

for some $\mu_0 \in B_2^6$; the assumption on the rank type of V implies that the rank of μ_0 and $\mu + \mu_0$ are both at least 4. We need to prove (i) $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$ and (ii) $B_3V = B_5$.

(i) $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$. Suppose that $a\mu = b\mu' \in B_2\mu \cap B_2\mu'$, for some $a, b \in B_2$. Let

$$b = \mu_1 + \lambda_1 x_7 + \lambda_2 x_8 + \epsilon x_7 x_8, \quad a = \mu_2 + \lambda_3 x_7 + \lambda_4 x_8 + \epsilon' x_7 x_8$$

where $\mu_1, \mu_2 \in B_2^6$, $\lambda_1, \lambda_2, \lambda_3, \lambda_4 \in B_1^6$ and $\epsilon, \epsilon' \in \mathbb{F}$. Then

$$\begin{aligned} 0 &= a\mu + b\mu' \\ &= (\mu_0\mu_1 + \mu_2\mu) + x_7(\mu_0\lambda_1 + \lambda_3\mu) \\ &\quad + x_8(\mu_0\lambda_2 + \lambda_4\mu) + x_7x_8(\mu_0\epsilon + \mu_1 + \epsilon'\mu) \end{aligned}$$

So

$$\epsilon\mu_0 + \mu_1 = \epsilon'\mu, \quad \mu_0\mu_1 = \mu_2\mu, \quad \lambda_3\mu = \lambda_1\mu_0, \quad \lambda_4\mu = \lambda_2\mu_0$$

Then $\lambda_1\lambda_3\mu = \lambda_1^2\mu_0 = 0$. Therefore $\lambda_1\lambda_3 \in \mathrm{Ann}(\mu) \cap B_2 = \{0, \mu\}$. But $\mu \neq \lambda_1\lambda_3$ since $\mathrm{rk}\,\mu = 6$, so $\lambda_1\lambda_3 = 0$. Suppose $\lambda_1 = \lambda_3 \neq 0$. Then

$\lambda_1(\mu + \mu_0) = 0$; but this is impossible since $\mathrm{rk}(\mu + \mu_0) \geq 4$. If $\lambda_1 \neq 0$ and $\lambda_3 = 0$ then we would have $\lambda_1\mu_0 = 0$ which is again impossible because $\mathrm{rk}(\mu_0) \geq 4$. A similar argument works for the case $\lambda_1 = 0$ and $\lambda_3 \neq 0$. Thus we must have $\lambda_1 = \lambda_3 = 0$. An analogous argument shows that $\lambda_2 = \lambda_4 = 0$ also. Therefore, $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = 0$.

Now consider the first two constraints: $\epsilon\mu_0 + \mu_1 = \epsilon'\mu, \mu_0\mu_1 = \mu_2\mu$. Consider the two cases:

$\epsilon' = 1$: Then $\epsilon\mu_0 + \mu_1 = \mu$. So $\mu_2\mu = \mu_0\mu_1 = \mu_0\mu$. Hence $\mu(\mu_0 + \mu_2) = 0$ and so $\mu_0 + \mu_2 \in \mathrm{Ann}(\mu) \cap B_2 = \{0, \mu\}$; that is, $\mu_2 \in \{\mu_0, \mu_0 + \mu\}$. So $a \in \{\mu', \mu' + \mu\}$ and $a\mu = \mu'\mu$ as required.

$\epsilon' = 0$: Then $\mu_1 = \epsilon\mu_0$, so $\mu_2\mu = \mu_0\mu_1 = 0$. Hence $\mu_2 \in \{0, \mu\}$ and $a\mu = 0$.

This proves that $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$.

(ii) $B_3V = B_5$. Recall that $B_3 = B_3^6 \oplus B_2^6x_7 \oplus B_2^6x_8 \oplus B_1^6x_7x_8$ so

$$B_3\mu = B_3^6\mu \oplus B_2^6\mu x_7 \oplus B_2^6\mu x_8 \oplus B_1^6\mu x_7x_8$$

Also

$$B_5 = B_5^6 \oplus B_4^6x_7 \oplus B_4^6x_8 \oplus B_3^6x_7x_8$$

It is easily verified directly that $B_3^6\mu = B_5^6$ (all degree 5 monomials can easily be realized as multiples of μ). Since $x_7\mu' = x_7\mu_0$,

$$B_3V \supset x_7B_2^6\mu + x_7B_2^6\mu' = (B_2^6\mu + B_2^6\mu_0)x_7 = B_4^6x_7$$

by Lemma 6.2. Similarly $B_3V \supset B_4^6x_8$.

Finally, if $a \in B_3^6$ then $a\mu' = a\mu_0 + ax_7x_8 \in B_3V$. But $a\mu_0 \in B_5^6 \subset B_3V$, so $ax_7x_8 \in B_3V$ also. Hence $B_3^6x_7x_8 \subset B_3V$. Putting all this together yields $B_5 = B_5^6 \oplus B_4^6x_7 \oplus B_4^6x_8 \oplus B_3^6x_7x_8 \subset B_3 \otimes V$, so $B_3V = B_5$ as claimed. Hence, all such Type A spaces are semi-regular. □

Theorem 7.8. *Let $\mu = x_1x_2 + x_3x_4 + x_5x_6$. Then*

(1) There are $11,796,480$ Type A semi-regular subspaces of B_2^8 containing μ which are of type $[6,8,8]$.
(2) There are $31,997,952$ Type A semi-regular subspaces of B_2^8 containing μ which are of type $[6,8,6]$.
(3) There are $20,643,840$ Type A semi-regular subspaces of B_2^8 containing μ which are of type $[6,6,6]$.

Proof. (1) If $V \ni \mu$ is of Type A, then there exist $\lambda, \lambda' \in \langle x_1, \ldots, x_6\rangle$ such that $V = \langle \mu, \mu' \rangle$ and

$$\mu' = \mu_0 + (\lambda' + x_7)(\lambda + x_8)$$

for some $\mu_0 \in \langle x_1, \ldots, x_6\rangle$. If V is of rank type $[6,8,8]$, then $\langle \mu, \mu_0\rangle$ must be of rank type $[6,6,6]$. The number of $[6,6,6]$ subspaces of B_2^6 is 13,332,480; the number of elements of B_2^6 of rank 6 is 13,880. So the number of $[6,6,6]$ subspaces of B_2^6 containing μ is

$$3 * 13,332,480/13,888 = 2,880$$

For each such subspace there are 2^{12} choices for λ_1 and λ_2, yielding a total of

$$2,880 * 2^{12} = 11,796,480$$

[6, 6, 6] subspaces of Type A containing μ. The numbers in (2) and (3) are found by a similar calculation using the number of [6,4,6] and [6,4,4] subspaces (54,246,528 and 69,995,520 respectively). □

This completes our analysis of the Type A case. We now move to the Type B case, which requires a little more work.

Lemma 7.9. *Suppose $\lambda, \lambda', \kappa, \kappa' \in B_1$ and λ and λ' are linearly independent. If $\lambda\kappa + \lambda'\kappa' = 0$, then $\kappa, \kappa' \in \langle \lambda, \lambda' \rangle$.*

Proof. We may assume that $\lambda = x_1$ and $\lambda' = x_2$. The result is then clear by considering the support of $x_1\kappa + x_2\kappa'$. □

Lemma 7.10. *Suppose that $\mu' = \mu_0 + \lambda x_7 + \lambda' x_8$ for some $0 \neq \mu_0 \in B_2^6$ and some linearly independent $\lambda, \lambda' \in B_1^6$. Then $\operatorname{rk} \mu' \geq 6$ if and only if $\mu_0 \notin B_1^6\lambda + B_1^6\lambda'$.*

Proof. Choose a complementary subspace W such that $B_1^6 = W \oplus \langle \lambda, \lambda' \rangle$ and write $\mu_0 = \alpha\lambda + \alpha'\lambda' + \nu$ where $\alpha, \alpha' \in B_1^6$ and $\nu \in W^2$. Then

$$\mu' = \nu + \lambda(\alpha + x_7) + \lambda(\alpha' +' x_8)$$

Let $W' = \langle \lambda, \lambda', \alpha + x_7, \alpha' + x_8 \rangle$. Since $B_1^8 = W \oplus W'$, $\operatorname{rk} \mu' = \operatorname{rk} \nu + 4$. Hence $\operatorname{rk} \mu' \geq 6$ if and only if $\operatorname{rk} \nu > 0$; that is, if and only if $\mu_0 \notin B_1^6\lambda + B_1^6\lambda'$. □

Theorem 7.11. *Suppose that $V = \langle \mu, \mu' \rangle$ where*

$$\mu = x_1x_2 + x_3x_4 + x_5x_6 \text{ and } \mu' = \mu_0 + \lambda x_7 + \lambda' x_8$$

for some $0 \neq \mu_0 \in B_2^6$ and some linearly independent $\lambda, \lambda' \in B_1^6$. Then V is semi-regular if and only if $\lambda\lambda'\mu_0 \notin B_2^6\mu$.

Proof. Suppose that $\lambda\lambda'\mu_0 \in B_2\mu$. We want to show that V is not semi-regular. We may assume that μ and μ' have rank at least 6 because otherwise V is not semi-regular by Theorem 7.1. Clearly $\lambda\lambda'\mu' \in B_2\mu \cap B_2\mu'$. We want to show that $\lambda\lambda'\mu' \notin \{0, \mu\mu'\}$. Suppose that $\lambda\lambda'\mu' = \mu\mu'$. Then $\lambda\lambda' + \mu \in \operatorname{Ann}(\mu') \cap B_2^6 = \{0, \mu'\}$ by Lemma 4.1. Hence $\lambda\lambda' \in \{\mu, \mu + \mu'\}$, contradicting the fact that both μ and $\mu + \mu'$ have rank at least 6. If $\lambda\lambda'\mu' = 0$, then $\lambda\lambda' \in \operatorname{Ann}(\mu') \cap B_2^6 = \{0, \mu'\}$, again yielding a contradiction because the linear independence property of λ and λ' implies that $\lambda\lambda' \neq 0$. So $B_2\mu \cap B_2\mu' \supsetneq \{0, \mu\mu'\}$ and V is not semi-regular by Lemma 7.3.

Now assume that $\lambda\lambda'\mu_0 \notin B_2\mu$. This implies that $\mu_0, \mu + \mu_0 \notin B_1^6\lambda + B_1^6\lambda'$, and hence, by Lemma 7.10, the ranks of μ' and $\mu' + \mu$ are at least 6. As before, we need to prove (i) $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$ and (ii) $B_3V = B_5$. Set $\Lambda = \langle \lambda, \lambda' \rangle$.

(i) $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$: Suppose $a\mu = b\mu' \neq 0$ where

$$a = \mu_2 + \lambda_1 x_7 + \lambda_2 x_8 + \epsilon' x_7 x_8, \quad b = \mu_1 + \lambda_7 x_7 + \lambda_8 x_8 + \epsilon x_7 x_8,$$

and $\mu_2, \mu_1 \in B_2^6, \lambda_1, \lambda_2, \lambda_7, \lambda_8 \in B_1^6, \epsilon, \epsilon' \in \mathbb{F}$. Equating the coefficients of $x_7 x_8$ on both sides of $a\mu = b\mu'$, yields

$$\epsilon'\mu = \epsilon\mu_0 + \lambda\lambda_8 + \lambda'\lambda_7.$$

So

$$\epsilon'\mu + \epsilon\mu' = \lambda(\epsilon x_7 + \lambda_8) + \lambda'(\epsilon x_8 + \lambda_7).$$

Since the right hand side has rank at most 4 and the rank of μ, μ' and $\mu + \mu'$ are all at least 6, this implies that $\epsilon = \epsilon' = 0$. Hence $\lambda\lambda_8 + \lambda'\lambda_7 = 0$, so by Lemma 7.9, $\lambda_7, \lambda_8 \in \Lambda$.

Thus

$$a = \mu_2 + \lambda_1 x_7 + \lambda_2 x_8, \quad b = \mu_1 + \lambda_7 x_7 + \lambda_8 x_8,$$

Comparing the coefficients of x_7, x_8 and the term that is purely contained in B_4^6 yields

$$\mu\lambda_1 = \mu_0\lambda_7 + \mu_1\lambda$$
$$\mu\lambda_2 = \mu_0\lambda_8 + \mu_1\lambda'$$
$$\mu_0\mu_1 = \mu\mu_2$$

Since $\lambda_7 \in \Lambda$, $\lambda_7\lambda \in \Lambda^2 = \{0, \lambda\lambda'\}$. If $\lambda_7\lambda = \lambda'\lambda$, then

$$\mu\lambda_1\lambda = \mu_0\lambda_7\lambda = \mu_0\lambda'\lambda$$

contradicting our assumption that $\mu_0\lambda\lambda' \notin B_2^6\mu$. Therefore $\lambda_7\lambda = 0$ and so $\lambda_7 \in \{0, \lambda\}$. Similarly we obtain $\lambda_8 \in \{0, \lambda'\}$ and $\lambda_7 + \lambda_8 \in \{0, \lambda + \lambda'\}$. Therefore

$$(\lambda_7, \lambda_8) = (0, 0) \text{ or } (\lambda, \lambda')$$

Since $\lambda_7\lambda = 0$, we also have $\mu\lambda_1\lambda = 0$. Since $\operatorname{rk}\mu = 6$, this implies $\lambda_1\lambda = 0$, and so $\lambda_1 \in \{0, \lambda\}$. Similarly we obtain $\lambda_2 \in \{0, \lambda'\}$ and $\lambda_1 + \lambda_2 \in \{0, \lambda + \lambda'\}$. Thus

$$(\lambda_1, \lambda_2) = (0, 0) \text{ or } (\lambda, \lambda')$$

Suppose $\lambda_1 = \lambda_2 = 0$. If $\lambda_7 = \lambda_8 = 0$, then $\lambda, \lambda' \in \operatorname{Ann}(\mu_1)$, so $\mu_1 \in \{0, \lambda\lambda'\}$. Since $b \neq 0$, we must have $\mu_1 \neq 0$, so $\lambda\lambda'\mu_0 = \mu_1\mu_0 = \mu\mu_2 \in B_2^6\mu$, a contradiction.

Now suppose that $(\lambda_7, \lambda_8) = (\lambda, \lambda')$. Then

$$(\mu_0 + \mu_1)\lambda = \mu_0\lambda_7 + \mu_1\lambda = 0 \text{ and } (\mu_0 + \mu_1)\lambda' = \mu_0\lambda_8 + \mu_1\lambda' = 0$$

so $\lambda, \lambda' \in \operatorname{Ann}(\mu_0 + \mu_1)$ and $\mu_0 + \mu_1 \in \{0, \lambda\lambda'\}$. If $\mu_0 + \mu_1 = 0$, then $b = \mu'$ and $b\mu' = 0$, contradicting our assumption. Thus $\mu_0 + \mu_1 = \lambda\lambda'$ so $b = \mu' + \lambda\lambda'$ and $\lambda\lambda'\mu_0 = (b + \mu')\mu' = a\mu \in B_2^6\mu$, again a contradiction.

Hence we must have $(\lambda_1, \lambda_2) = (\lambda, \lambda')$. In this case

$$\mu\lambda = \mu_0\lambda_7 + \mu_1\lambda$$
$$\mu\lambda' = \mu_0\lambda_8 + \mu_1\lambda'$$

If $(\lambda_7, \lambda_8) = (0, 0)$, then $\operatorname{Ann}(\mu + \mu_1)$ contains Λ and therefore $\mu + \mu_1 \in \{0, \lambda\lambda'\}$. If $\mu + \mu_1 = \lambda\lambda'$, then $\mu_1 = \mu + \lambda\lambda'$ and so $\mu\mu_2 = \mu_0(\mu + \lambda\lambda')$ which would imply $\lambda\lambda'\mu_o \in B_2^6\mu$, a contradiction. So $\mu + \mu_1 = 0$, in which case $b = \mu$ and $b\mu = \mu\mu'$ as required.

If $\lambda_7 = \lambda$ and $\lambda_8 = \lambda'$, then $\mathrm{Ann}(\mu + \mu_1 + \mu_0)$ contains Λ and therefore $\mu + \mu_1 + \mu_0 \in \{0, \lambda\lambda'\}$. If $\mu + \mu_1 + \mu_0 = \lambda\lambda'$, then $\mu_1 = \mu + \mu_0 + \lambda\lambda'$ and so $\mu\mu_2 = \mu_0(\mu + \mu_0 + \lambda\lambda')$ which again implies $\lambda\lambda'\mu_o \in B_2^6\mu$, a contradiction. So $\mu + \mu_1 + \mu_0 = 0$, or $\mu = \mu_0 + \mu_1$. Hence

$$\begin{aligned} b\mu' &= (\mu_1 + \lambda x_7 + \lambda' x_8)(\mu_0 + \lambda x_7 + \lambda' x_8) \\ &= \mu_1\mu_0 + \lambda(\mu_0 + \mu_1)x_7 + \lambda'(\mu_0 + \mu_1)x_8 \\ &= (\mu_0 + \mu_1)(\mu_0 + \lambda x_7 + \lambda' x_8) \\ &= \mu\mu' \end{aligned}$$

Thus we have proved that $B_2\mu \cap B_2\mu' = \{0, \mu\mu'\}$

In this case $\{\lambda, \lambda'\}$ is linearly independent so we may extend $\{\lambda, \lambda'\}$ to a basis $\{\lambda, \lambda', y_1, y_2, y_3, y_4\}$ for B_2^6. Let $Y = \mathrm{Span}(y_1, y_2, y_3, y_4)$. Then we have that after a possible change of the x_i basis, $\mu' = \mu_0 + \lambda x_7 + \lambda' x_8$ where $\mu_0 \in Y$.

(ii) $B_3V = B_5$: Recall, as in the previous proof, that $B_3 = B_3^6 \oplus x_7B_2^6 \oplus x_8B_2^6 \oplus x_7x_8B_1^6$; that

$$B_5 = B_5^6 \oplus B_4^6x_7 \oplus B_4^6x_8 \oplus B_3^6x_7x_8$$

and that $B_5^6 = B_3^6\mu \subset B_3V$. Now $\dim B_2^6\mu = 14 = \dim B_4^6 - 1$, so the assumption that $\lambda\lambda'\mu' = \lambda\lambda'\mu_0 \notin B_2^6\mu$ implies that $B_2^6V \supset B_4^6$. So

$$B_3V \supset (B_2^6x_7 + B_2^6x_8)V = B_2^6Vx_7 + B_2^6Vx_8 \supset B_4^6x_7 + B_4^6x_8.$$

Thus it remains to show that $B_3V \supset B_3^6x_7x_8$. For $b \in B_2^6$ we have that

$$bx_7\mu' = b\mu_0x_7 + b\lambda'x_7x_8$$

Since $b\mu_0x_7 \in B_4x_7 \subset B_3V$, this implies that $b\lambda'x_7x_8 \in B_3V$. A similar argument for λ yields that $B_3V \supset (B_2^6\lambda + B_2^6\lambda')x_7x_8$. Also $B_3V \supset B_1^6x_7x_8\mu' = B_1^6\mu_0x_7x_8$, and $B_3V \supset B_1^6x_7x_8\mu$. Hence

$$B_3V \supset (B_1^6\mu_0 + B_2^6\lambda + B_2^6\lambda' + B_1^6\mu)x_7x_8$$

Thus it suffices to show that $B_1^6\mu_0 + B_2^6\lambda + B_2^6\lambda' + B_1^6\mu = B_3^6$. Then we may write $\mu = \nu + \lambda a + \lambda a'$ where $\nu \in Y$ and $a, a' \in B_1^6$. Then $B_1^6\mu_0 + B_2^6\lambda + B_2^6\lambda' + B_1^6\mu = B_3^6$ is equivalent to $Y\mu_0 + Y\nu = Y^3$. Suppose that $Y\mu_0 + Y\nu \neq Y^3$. Then μ_0, ν and $\mu_0 + \nu$ all have rank 2, so we may assume that, after an appropriate change of basis, that $\mu_0 = y_1y_2$ and $\nu = y_1y_3$. In this case

$$\mu = y_1y_3 + \lambda a + \lambda' a'$$

and since μ has rank 6, $y_1, y_3, \lambda, a, \lambda', a'$ must form a basis for B_1^6. Let $A = \mathrm{Span}(a, a')$. Then

$$\Lambda y_1\mu = \Lambda y_1(\lambda a + \lambda' a') = y_1\lambda\lambda' A$$

Since $\lambda\lambda'\mu = y_1\lambda\lambda' y_3$, this yields that

$$B_2^6\mu \supset \Lambda y_1\mu + \mathbb{F}\lambda\lambda'\mu = y_1\lambda\lambda'(A + \mathbb{F}y_3) = y_1\lambda\lambda' B_1^6 = (y_1 B_1^6)\lambda\lambda'$$

Hence $\mu_0\lambda\lambda' = y_1 y_2\lambda\lambda' \in B_2^6\mu$, contrary to assumption. □

Lemma 7.12. *Let $\mu = x_1x_2 + x_3x_4 + x_5x_6 \in B_2^6$ and let λ, λ' be linearly independent elements of B_1^6. Then there exists a $\mu_1 \in B_2^6$ such that $\lambda\lambda'\mu_1 \notin B_2\mu$.*

Proof. Note first that $\dim B_2^6\mu = 15 - 1 = 14$ by Lemma 4.1 and $\dim B_4^6 = 15$, so $B_2^6\mu \subsetneq B_4^6$. On the other hand if $V = \langle \mu, \lambda\lambda' \rangle$, then by Lemma 6.2 we have that $B_2^6 V = B_4^6$. Hence there must exist a $\mu_1 \in B_2^6$ with $\mu_1\lambda\lambda' \notin B_2^6\mu$. □

Theorem 7.13. *Let $\mu = x_1x_2 + x_3x_4 + x_5x_6 \in B_2^6$. Let $\mathcal{T}_B$ be the set of all non-induced two dimensional subspaces of B_2^8 that are Type B with respect to μ. For each pair of linearly independent elements $\lambda, \lambda' \in B_1^6$ choose a $\mu_1 \in B_2^6$ such that $\lambda\lambda'\mu_1 \notin B_2\mu$. Define $\Phi : \mathcal{T}_B \to \mathcal{T}_B$ by*

$$\begin{aligned}\Phi(\{0, \mu, &\mu_0 + \lambda x_7 + \lambda' x_8, \mu + \mu_0 + \lambda x_7 + \lambda' x_8\}) \\ &= \{0, \mu, \mu_0 + \mu_1 + \lambda x_7 + \lambda' x_8, \mu + \mu_0 + \mu_1 + \lambda x_7 + \lambda' x_8\}\end{aligned}$$

Then $\Phi^2 = I$ and $\Phi(V)$ is semi-regular if and only if V is not semi-regular. Hence there is the same number of semi-regular and non-semi-regular spaces of Type B with respect to μ. In particular, there are $63*62*2^{13} = 31,997,952$ semi-regular subspaces of Type B.

Proof. Since $\dim B_4^6/B_2^6\mu = 1$, we have that $\lambda\lambda'\mu_0 \in B_2^6\mu$ if and only if $\lambda\lambda'(\mu_0 + \mu_1) \notin B_2^6\mu$. In particular there are $31,997,952$ semi-regular subspaces of type B with respect to μ. The number of choices for λ and λ' is $63 * 62$; the number of choices for μ_0 is 2^{15} and these come in pairs, $\{\mu_0, \mu_0 + \mu\}$ which generate the same subspace. So the total number of type B subspaces is $63 * 62 * 2^{14}$, and half of these are semi-regular. □

Theorem 7.14. *Let $\lambda, \lambda', \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6, x_7, x_8$ be a basis for B_1^8 and let $W = \langle \lambda, \lambda', \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6 \rangle$. Let $\mu' = \epsilon_3\epsilon_4 + \epsilon_5\epsilon_6 + \lambda x_7 + \lambda' x_8$ and let $\mu = \nu + a\lambda + b\lambda' + \eta\lambda\lambda' \in W^2$ be an element of rank 6 for some $a, b \in \langle \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6 \rangle$ and $\nu \in \langle \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6 \rangle^2$. Then the two dimensional vector space $V = \langle \mu, \mu' \rangle$ is semi-regular if and only if $\nu(\epsilon_3\epsilon_4 + \epsilon_5\epsilon_6) \neq 0$.*

Proof. Let $\mu_0 = \epsilon_3\epsilon_4 + \epsilon_5\epsilon_6$. Suppose that V is not semi-regular. then by an earlier result, we know that $\lambda\lambda'\mu_0 = \gamma\mu$ for some $\gamma = e + c\lambda + d\lambda' + \eta'\lambda\lambda' \in W$. Now

$$\begin{aligned}\gamma\mu &= (\nu + a\lambda + b\lambda' + \eta\lambda\lambda')(e + c\lambda + d\lambda' + \eta'\lambda\lambda') \\ &= \nu e + (ae + \nu c)\lambda + (d\nu + eb)\lambda' + (\eta'\nu + \eta e + cb + ad)\lambda\lambda'\end{aligned}$$

Comparing coefficients yields

$$\begin{aligned}\mu_0 &= \eta'\nu + \eta e + cb + ad \\ 0 &= \nu e \\ 0 &= ae + c\nu \\ 0 &= be + d\nu\end{aligned}$$

So

$$\begin{aligned}\nu\mu_0 &= (\eta'\nu + \eta e + cb + ad)\nu \\ &= bc\nu + ad\nu = b(ae) + a(be) = 0\end{aligned}$$

Conversely assume that $\nu\mu_0 = 0$. Suppose first that $\eta = 1$. Then $\lambda\lambda' = \mu + \nu + a\lambda + b\lambda'$ and so

$$\lambda\lambda'\mu_0 = (\mu + \nu + a\lambda + b\lambda')\mu_0 = \mu_0\mu + (a\lambda + b\lambda')\mu_0$$

Now $\mu = (\nu + ab) + (\lambda + b)(\lambda' + a)$ and so $\operatorname{rk}(\nu + ab) = 4$, since $\operatorname{rk}\mu = 6$. Let $U = \langle \epsilon_3, \ldots, \epsilon_6 \rangle$. Since $\operatorname{rk}\mu_0 = 4$ also we have $U(\nu + ab) = U\mu_0$. So there exist $c, d \in U$ such that $a\mu_0 = c(\nu + ab)$ and $b\mu_0 = d(\nu + ab)$. But then

$$\begin{aligned}[(\lambda + b)c + (\lambda' + a)d]\mu &= (\lambda + b)c(\nu + ab) + (\lambda' + a)d(\nu + ab) \\ &= (\lambda + b)a\mu_0 + (\lambda' + a)b\mu_0 \\ &= (a\lambda + b\lambda')\mu_0\end{aligned}$$

So $\lambda\lambda'\mu_0 \in B_2\mu$ and V is not semi-regular.

Now suppose $\eta = 0$. Then, $\mu = \nu + a\lambda + b\lambda'$. If $a = b$, $\mu = \nu + a(\lambda + \lambda')$ is expressible in five variables, but $\operatorname{rk}(\mu) = 6$, so $a \neq b$. Then we can extend a, b to a basis a, b, c, d for $\langle \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6 \rangle$. Since μ is rank 6, it must have a term not divisible by a or b, so $cd \in \operatorname{Supp}(\nu) \subset \operatorname{Supp}(\mu)$ in the a, b, c, d basis. Depending on if ac, ad, bc, bd, ab are in $\operatorname{Supp}(\nu)$, we have $\mu = \nu + a\lambda + b\lambda' = (c + \epsilon_1 a + \epsilon_1' b)(d + \epsilon_2 a + \epsilon_2' b) + \epsilon ab + a\lambda + b\lambda'$, for some $\epsilon_1, \epsilon_1', \epsilon_2, \epsilon_2', \epsilon \in \mathbb{F}$. Making a coordinate transformation $c \to c + \epsilon_1 a + \epsilon_1' b, d \to d + \epsilon_2 a + \epsilon_2' b$, we get $\mu = cd + \epsilon ab + a\lambda + b\lambda'$, where $\langle a, b, c, d \rangle = \langle \epsilon_3, \epsilon_4, \epsilon_5, \epsilon_6 \rangle$ and $\epsilon \in \{0, 1\}$ with $\nu = cd + \epsilon ab$. Note that

$$(\lambda' + \epsilon a)c\mu = \lambda\lambda' ac \in B_2\mu$$

Likewise,

$$\lambda\lambda'\langle ac, ad, bc, bd \rangle \in B_2\mu$$

Also,

$$\lambda\lambda'\mu = \lambda\lambda'(\epsilon ab + cd) \in B_2\mu$$

In both cases, whether $\epsilon = 0$ or 1, we see therefore that

$$B_2\mu \supseteq \lambda\lambda'\langle ac, ad, bc, bd, \epsilon ab + cd \rangle = \lambda\lambda' \operatorname{Ann}(\epsilon ab + cd) = \lambda\lambda' \operatorname{Ann}(\nu) \ni \lambda\lambda'\mu_0$$

The last inclusion is because $\nu\mu_0 = 0$ implies $\mu_0 \in \operatorname{Ann}(\nu)$. Hence, $\lambda\lambda'\mu_0 \in B_2\mu$, and V is not semi-regular. □

Lemma 7.15. *Let $a, b \in B_1^4$. Then the following are equivalent*

(1) $\operatorname{rk}(x_1x_2 + ax_5 + bx_6) = 6$

(2) x_1, x_2, a, b, x_5, x_6 *are a basis for* B_2^6
(3) x_1, x_2, a, b *are a basis for* B_2^4
(4) $\operatorname{rk}(x_1x_2 + ab) = 4$
(5) $\operatorname{rk}(x_1x_2 + ax_5 + bx_6 + x_5x_6) = 6$

Moreover there are 96 possible such choices for the pair a, b.

Proof. The equivalence of the first four conditions is straightforward. For the last equivalence we note that

$$x_1x_2 + ax_5 + bx_6 + x_5x_6 = x_1x_2 + ab + (a + x_6)(b + x_5)$$

Clearly the number of choices of a and b satisfying (3) is $(2^4 - 4)(2^4 - 8) = 96$. □

Lemma 7.16. *Let* $\mu \in B_2^4$ *be an element of rank 4 and let* $N = \{\nu \in B_2^4 \mid \nu\mu \neq 0\}$. *Then* $|N| = 32$ *and* N *contains 12 elements of rank 4 and 20 elements of rank 2. Moreover, if* $\nu \in N$, *then* $\operatorname{rk}\nu = \operatorname{rk}\nu + \mu$.

Proof. Let $V = \langle \mu, \nu \rangle$. Then $\nu \in N$ if and only if $V^2 \neq 0$. The two dimensional subspaces of B_2^4 of types $[4, 4, 4]$, $[4, 4, 2]$ and $[4, 2, 2]$ are equivalent up to change of basis to the spaces

$$\begin{aligned}
[4,4,4]:&\quad \{0, x_1x_2 + x_3x_4, x_1x_2 + x_1x_3 + x_2x_4, x_3x_4 + x_1x_3 + x_2x_4\}\\
[4,4,2]:&\quad \{0, x_1x_2 + x_3x_4, x_1x_3, x_1x_3 + x_1x_2 + x_3x_4\}\\
[4,2,2]:&\quad \{0, x_1x_2 + x_3x_4, x_1x_2, x_3x_4\}.
\end{aligned}$$

Thus $V^2 \neq 0$ if and only if V is of type $[4, 4, 4]$ or $[4, 2, 2]$. It follows immediately that $\operatorname{rk}\nu = \operatorname{rk}\nu + \mu$. There are 6 subspaces of type $[4, 4, 4]$ containing a given μ and 10 of type $[4, 2, 2]$. Thus N contains 12 elements of rank 4 and 20 elements of rank 2. □

Lemma 7.17. *Let* $\mu \in B_2^8$ *have rank 6. Then there are* $63 * 62 * 2^9 * 28$ *elements* μ' *of rank 8 such that* $\langle \mu, \mu' \rangle$ *is of Type B with respect to* μ.

Proof. We may suppose that μ has the usual form and that

$$\mu' = \mu_0 + \lambda x_7 + \lambda' x_8$$

where λ, λ' are linearly independent. Now choose a subspace $W \subset B_1^6$ such that $B_1^6 = W \oplus (\mathbb{F}\lambda + \mathbb{F}\lambda')$. In this case we can write $\mu_0 = \nu_0 + \kappa\lambda + \kappa'\lambda' + \epsilon\lambda\lambda'$ where $\nu_0 \in W^2$ and $\kappa, \kappa' \in W$. If $\epsilon = 0$, then

$$\mu' = \nu_0 + \lambda(x_7 + \kappa) + \lambda'(x_8 + \kappa')$$

and this element has rank 8 if and only if ν_0 has rank 4. If $\epsilon = 1$,

$$\mu' = \nu_0 + \lambda(x_7 + \kappa + \lambda') + \lambda'(x_8 + \kappa')$$

Again this has rank 8 if and only if ν_0 has rank 4. In each case there are $63*62$ choices for λ, λ', 2^8 choices for κ and κ' and 28 choices for ν_0 yielding a total of $63 * 62 * 2^9 * 28$ choices for μ'. □

Lemma 7.18. *Let* ν *be a rank 4 element of* B_2^4 *such that* $\nu \notin B_1^4 x_1 + B_1^4 x_2$. *Then there exists a basis* x_1, x_2, y_3, y_4 *of* B_1^4 *such that* $\nu = x_1x_2 + y_3y_4$.

Theorem 7.19. *Consider two dimensional subspaces of the form* $V = \langle \mu, \mu' \rangle$ *where* $\mu \in B_2^6$ *has rank 6;* $\mu' = \mu_0 + \lambda x_7 + \lambda' x_8$ *for some* $\mu_0 \in B_2^6$ *and linearly independent* $\lambda, \lambda' \in B_1^6$ *and* $\operatorname{rk} \mu' = 8$. *Then there are*

(1) $63 * 62 * 2^9 * 28 * 12 * 256/2$ *such subspaces of type* $[6, 8, 8]$.
(2) $63 * 62 * 2^9 * 28 * 20 * 192$ *such subspaces of type* $[6, 6, 8]$*;*

Proof. As in the proof of Lemma 7.17, after applying an automorphism that fixes B_1^6 we may assume that there is a subspace $W \subset B_1^6$ such that $B_1^6 = W \oplus (\mathbb{F}\lambda + \mathbb{F}\lambda')$ and $\mu_0 \in W^2$; so $\operatorname{rk}(\mu_0) = 4$. In this case $\mu = \nu + a\lambda + b\lambda' + \epsilon\lambda\lambda'$ where $\nu \in W^2$, $a, b \in W$ and $\epsilon \in \mathbb{F}$. By Theorem 7.14, V is semi-regular if and only if $\nu\mu_0 \neq 0$. By Lemma 7.16, there are 12 options for ν of rank 4 and 20 options of rank 2. Again by Lemma 7.16, we see that if $\operatorname{rk} \nu = 4$, then V is of type $[6, 8, 8]$ and if $\operatorname{rk} \nu = 2$. then V is of type $[6, 6, 8]$. Now we use Lemma 7.15 to count the number of possible μ for which V is semi-regular of each type for our fixed μ'. We consider 4 cases

(i) $\operatorname{rk} \nu = 2$, $\epsilon = 0$. Thus $\mu = \nu + a\lambda + b\lambda'$ and by Lemma 7.15 there are 96 choices for a and b which yield $\operatorname{rk} \mu = 6$.

(ii) $\operatorname{rk} \nu = 2$, $\epsilon = 1$. Thus $\mu = \nu + a\lambda + b\lambda' + \lambda\lambda' = \nu + ab + (\lambda + b)(\lambda' + a)$. In this case $\operatorname{rk} \mu = 6$ if and only if $\operatorname{rk} \nu + ab = 4$. Again by the Lemma there are 96 choices for this.

Thus in the $[6, 6, 8]$ case, for any given μ' there are 20 choices for ν and 192 choice for a, b and ϵ, proving (2).

(iii) $\operatorname{rk} \nu = 4$, $\epsilon = 0$. Again $\mu = \nu + a\lambda + b\lambda'$. Note that a and b must be linearly independent or μ is not of rank 6. Also $\nu \notin \langle a, b \rangle B_1^4$, otherwise $\operatorname{rk} \mu < 6$. So by Lemma 7.18 $\nu = ab + y_3 y_4$ where a, b, y_3, y_4 is a basis for W. Thus $\langle \nu, ab \rangle$ is a $[4, 2, 2]$ space containing ν. There are ten such subspaces for each ν and 12 choices for ν yielding a total of 120 choices for μ.

(iv) $\operatorname{rk} \nu = 4$, $\epsilon = 1$. Here $\mu = \nu + ab + (\lambda + b)(\lambda' + a)$. In this case $\operatorname{rk} \mu = 6$ if and only if $\operatorname{rk} \nu + ab = 4$. If $ab = 0$, this is always true and there are 46 ways to choose a and b such that $ab = 0$. If $ab \neq 0$, this holds if and only if $\langle \nu, ab \rangle$ is of type $[4, 4, 2]$. There are 15 such spaces containing a given rank for element, so 15 choices for ab, for which there are 6 different ways of choosing a and b. This yields 136 possibilities for μ in this case.

□

Corollary 7.20. *Let* $\mu \in B_2^8$ *have rank 6. Then*

(1) There are $6, 193, 152$ *2D semi-regular subspaces of* B_2^8 *of type* $[6, 8, 8]$ *which are Type B with respect to* μ.
(2) There are $15, 482, 880$ *2D semi-regular subspaces of* B_2^8 *of type* $[6, 8, 6]$ *which are Type B with respect to* μ.
(3) There are $10, 321, 920$ *2D semi-regular subspaces of* B_2^8 *of type* $[6, 6, 6]$ *which are Type B with respect to* μ.

Proof. (1) Let $\mathcal{V}$ be the set of two dimensional subspaces of the form in the Theorem which are of rank type $[6, 8, 8]$; that is, $V = \langle \mu, \mu' \rangle$ where $\mu \in B_2^6$ and $\mu' = \mu_0 + \lambda x_7 + \lambda' x_8$ for some $\mu_0 \in B_2^6$ and linearly independent

$\lambda, \lambda' \in B_1^6$. Let $\mathcal{V}_\mu$ be the subset of $\mathcal{V}$ consisting of spaces containing μ. Since $GL(B_1^6)$ acts transitively on the set of all rank 6 elements of B_2^6, we have that $\mathcal{V} = \bigsqcup \mathcal{V}_{\sigma(\mu)}$. Thus $|\mathcal{V}_\mu| = |\mathcal{V}|/13888$, yielding the claimed number. Similarly for part (2). For part (3), notice that the number of semi-regular subspaces of Type B is $31,997,952$ by Theorem 7.13. Since these have either rank type $[6,8,8], [6,6,8]$ or $[6,6,6]$, the number of the latter type is

$$31,997,952 - 6,193,152 - 15,482,880 = 10,321,920$$

□

Corollary 7.21. *Let $\mu = x_1x_2 + x_3x_4 + x_5x_6$. Then*

(1) There are $17,989,632$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,8,8]$ containing μ.
(2) There are $47,480,832$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,8,6]$ containing μ.
(3) There are $30,965,760$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,6,6]$ containing μ.

Proof. The number of such spaces is just the sum of the numbers in Theorem 7.8, and Corollary 7.20. □

Corollary 7.22. *There are*

(1) $2,697,022,899,486,720$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,8,8]$
(2) $3,559,185,957,519,360$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,8,6]$
(3) $1,547,472,155,442,200$ two-dimensional semi-regular subspaces of B_2^8 of type $[6,6,6]$

Proof. For any element of B_2^8 of rank 6, there is an automorphism $\sigma \in \mathrm{GL}(B_1^8)$ such that $\sigma(\tilde{\mu}) = \mu$. This automorphism then induces a bijection between the set of semi-regular subspaces of B_2^8 of type $[6,8,6]$ containing $\tilde{\mu}$ and the set of semi-regular subspaces of B_2^8 of type $[6,8,6]$ containing μ. Since there are $149,920,960$ elements of B_2^8 of rank 6, the total number of semi-regular subspaces of B_2^8 of type $[6,8,6]$ is

$$\frac{47,480,832 * 149,920,960}{2} = 3,559,185,957,519,360$$

The other cases are handled similarly. □

7.1. **Approximation of $p_{8,2}$.** The case when $\mathrm{Rk}\, V = [8,8,8]$ seems to be even more complex than the Type B case above. Thus we content ourselves with an approximation of $p_{8,2}$ in this case.

Theorem 7.23. *Let $p_{8,2}$ be the proportion of two dimensional subspaces of B_2^8 which are semi-regular. Then*

$$0.65 \leq p_{8,2} \leq 0.72$$

Proof. We are able to determine the semi-regularity of all but the $888,431,072,772,096$ spaces of rank type $[8,8,8]$. Using Corollary 7.22 we obtain that the number $sr(8,2)$ of semi-regular 2 dimensional suspaces satisfies

$$7,803,681,012,449,280 \leq sr(8,2) \leq 8,692,112,085,221,376$$

Dividing by the total number of 2 dimensional subspaces, $12,009,598,872,103,595$ yields the claimed bounds. □

8. Hilbert Polynomials

An even more fine-grained understanding can be obtained by looking at the possible Hilbert polynomials that can arise for B/BV. We list here (without proof) a complete description of the Hilbert polynomials that can arise in the cases $n = 4, 5$ and 6. The main determining factor is the rank-type and whether or not the space is induced.

Type	Number	$H_V(z)$
$[2,2,2]$	105	$1+4z+4z^2+z^3$
$[2,2,4]$	280	$1+4z+4z^2$
$[2,4,4]$	210	$1+4z+4z^2$
$[4,4,4]$	56	$1+4z+4z^2$
Total	651	

Table 5. Hilbert polynomials of B/BV by rank type when $n = 4$

Rank	Type	Number	$H_V(z)$
$[2,2,2]$		1,085	$1+5z+8z^2+5z^3+z^4$
$[2,2,4]$		8,680	$1+5z+8z^2+4z^3$
$[2,4,4]$	i	6,510	$1+5z+8z^2+4z^3$
$[2,4,4]$	ni	52,080	$1+5z+8z^2+2z^3$
$[4,4,4]$	i	1,736	$1+5z+8z^2+4z^3$
$[4,4,4]$	ni	104,160	$1+5z+8z^2+z^3$
Total		174,251	

Table 6. Decomposition of the Grassmanian by Rank Type for $n = 5$

When $n = 4$ the situation is simple. When $n = 5$ we begin to see the distinction between the induced and non-induced cases. When $n = 6$, more subtle distinctions begin to appear. In the types column we have

- i4: V is induced from a 4 dimensional subspace
- i5: V is induced from a 5 dimensional subspace
- nin: V is not induced but not semi-regular
- nis: V is not induced and is semi-regular

Rank	Type	Number	$H_V(z)$
$[2,2,2]$		9,765	$1+6t+13t^2+13t^3+6t^4+t^5$
$[2,2,4]$		182,280	$1+6t+13t^2+13t^3+4t^4$
$[2,4,4]$	i4	136,710	$1+6t+13t^2+13t^3+4t^4$
$[2,4,4]$	i5	3,281,040	$1+6t+13t^2+10t^3+2t^4$
$[2,4,6]$		4,666,368	$1+6t+13t^2+10t^3$
$[2,6,6]$		2,187,360	$1+6t+13t^2+10t^3$
$[4,4,4]$	i4	36,456	$1+6t+13t^2+13t^3+4t^4$
$[4,4,4]$	i5	6,562,080	$1+6t+13t^2+9t^3+t^4$
$[4,4,4]$	nin	8,749,440	$1+6t+13t^2+8t^3+t^4$
$[4,4,4]$	nis	15,554,560	$1+6t+13t^2+8t^3$
$[4,4,6]$		69,995,520	$1+6t+13t^2+8t^3$
$[4,6,6]$		54,246,528	$1+6t+13t^2+8t^3$
$[6,6,6]$		13,332,480	$1+6t+13t^2+8t^3$
Total		178,940,587	

TABLE 7. Hilbert Series by Rank and Type when $n = 6$

9. Conclusion

We conducted a detailed study of the semi-regularity of two dimensional quadratic spaces. We found the following values for $p_{n,2}$, the proportion of quadratic subspaces that were semi-regular.

n	3	4	5	6	7	8	≥ 9
$p_{n,2}$	1.00	0.84	0.00	0.86	0.00	$[0.65, 0.72]$	0.00

TABLE 8. The proportion $p_{n,2}$ of 2-dimensiion subspaces of B_2 that are semi-regular

Our hope was that this study would shed some light which would enable progress towards two of the most glaring open questions concerning semi-regularity: a) do there exist semi-regular sequences of quadratic element for all n? and b) is $\lim_{n\to\infty} p_{n,n} = 1$; i.e., are most sequences of n quadratic elements in n variables semi-regular? On the positive side, the rank type is an invariant whihc can be used to establish certain results easily. It seems possible that the answer to a) can be found by considering speciifc spaces of high rank type. On the other hand the table of Hilbert series in the case $n = 6$ suggest that getting the Hilbert series exactly right is a hard thing to control. While most spaces seem to be close to being semi-regular (in the sense that their Hilbert series are close to $T_{n,m}(z)$), it appears that it will be a highly non-trivial problem to prove the exact match of dimensions in each degree.

For most applications, it is sufficient to show that the degree of the Hilbert polynomial is the same as that of a semi-regular system. Proving this should be significantly easier and would give a more useful result from the point of view of applications. Thus a weaker but more accessible conjecture would be that for "most" m-dimensional subspaces $B_{D-2}V = B_V$ for $D = D_{n,m}$. For instance we are able to prove this result in the one case that we were not able to establish semi-regularity - spaces of rank type $[8, 8, 8]$ when $n = 8$.

References

[1] M. Bardet, *Étude des systèmes algébriques surdéterminés. Applications aux codes correctuers et la cryptographie.* PhD thesis, Université Paris VI, Décembre 2004.

[2] M. Bardet, J.-C. Faugère, B. Salvy and B.-Y. Yang, *Asymptotic Expansion of the Degree of Regularity for Semi-Regular Systems of Equations*, MEGA 2005, Sardinia, Italy

[3] J. Ding, T. J. Hodges, *Inverting the HFE systems is quasipolynomial for all fields.* In: Advances in Cryptology - Crypto 2011, Lecture Notes in Computer Science 6841, pp 724-742, Springer, Berlin 2011.

[4] J. Ding, T. J. Hodges, V. Kruglov, D. Schmidt, S. Tohaneanu, *Growth of the ideal generated by a multivariate quadratic function over GF(3)*, J. of Algebra and Its Applications, 12 (2013), 1250219-1 to 23.

[5] V. Dubois, N. Gama, *The degree of regularity of HFE systems.* In: Abe, M. (ed.) Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security. LNCS, vol. 6477, pp. 557-576. Springer, Berlin (2010)

[6] T. J. Hodges, C. Petit and J. Schlather, *First Fall Degree and Weil Descent*, Finite Fields and Their Applications 30 (2014), 155-177.

[7] T. J. Hodges and S. D. Molina, *Homological Characterization of bounded $\mathbb{F}_2$-regularity*, Cryptology ePrint Archive, Report ****/***

[8] T. J. Hodges, S. D. Molina and J. Schlather, *On the existence of homogeneous semi-regular sequences in $\mathbb{F}_2[X_1, \ldots, X_n]/(X_1^2, \ldots, X_n^2)$*, Journal of Algebra 476 (2017): 519-547.

[9] A. Pott, K-U. Schmidt, Y. Zhou, *Pairs of quadratic forms over Finite Fields*, Elec. J. Combin 23(2) (2016), #P2.8

[10] I. Semaev and A. Tenti, *Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Gröbner bases*, J. Algebra 565, 2021, pp 651-674

Appendix A. The General Upper Bound

Let V be an m-dimensional graded subspace of B. Let $\{\mu_1, \ldots, \mu_m\}$ be a homogeneous basis for V and set $d_i = \mu_i$. If we assume that $d_1 \leq \cdots \leq d_m$ then the vector $\underline{d} = (d_1, \ldots, d_m)$ is independent of the choice of homogeneous basis. For such a vector $\underline{d} = (d_1, \ldots, d_m)$ we define

$$T_{n,\underline{d}}(z) = \left[\frac{(1+z)^n}{\prod_i (1+z^{d_i})} \right]$$

and

$$D_{n,\underline{d}} := \deg T_{n,\underline{d}}(z)$$

Denote the Hilbert series of the quotient ring B/BV by $HS_V(z)$. We say the space V is semi-regular if $HS_V(z) = T_{n,\underline{d}}(z)$.

Theorem A.1. *Let V be a graded subspace of B^n with degree vector $\underline{d}$ and let $d = \sum_i d_i$. If $n \geq D_{n,\underline{d}} + d$, then V is not semi-regular.*

Proof. Let $B = \{\mu_1, \ldots, \mu_m\}$ be a basis for V. Choose an element ξ of BV of maximal degree. Clearly $\deg \xi \leq d$ and $\xi \mu_i = 0$ for all i. Let $D = D_{n,\underline{d}}$. If V is semi-regular, then

$$B_D = \sum_i B_{D-d_i} \mu_i$$

But then

$$\xi B_d = \xi \sum_i B_{D-d_i} \mu_i = \sum_i B_{D-d_i} \xi \mu_i = 0$$

This implies that $\xi \in B_{\deg \xi} \cap \operatorname{Ann} B_D = 0$. So Lemma 3.2 implies that $n < D + \deg \xi \leq D + d$. Thus if $n \geq D + d$, V can not be semi-regular. ☐

Email address, Tim Hodges: `timothy.hodges@uc.edu`

University of Cincinnati, Cincinnati, OH 45221-0025, USA

Email address, Hari Iyer: `hiyer@college.harvard.edu`

Harvard College, Cambridge, MA 02138