University of Wrocław

Faculty of Mathematics and Computer Science

Mathematical Institute

Uniwersytet Wrocławski

Wydział Matematyki i Informatyki

Instytut Matematyczny

Jakub Kamiński

Additive aspects of ideal multiplication in rings

Bachelor's thesis
written under the supervision of
dr hab. Jan Dymara

Praca licencjacka
napisana pod kierunkiem
dr hab. Jana Dymary

Abstract:

The ideal product AB in a ring is defined as the set of finite sums of products of the form ab. The naivety of a pair of ideals A, B is defined as the smallest length of such sum needed to get the whole AB. The following thesis contains the definition of naivety and the related based naivety, basic lemmas regarding both, examples calculated in various rings, the conclusions drawn from attempts to solve the problem, most promising methods, and related problems. Each section also contains a commentary explaining its point and other non-tangible results of work on the problem of naivety.

Streszczenie:

Iloczyn ideałów w pierścieniu definiowany jest przez sumy skończone elementów iloczynu kompleksowego tych ideałów. Przez naiwność pary ideałów będziemy rozumieć najmniejszą długość takich sum potrzebną do otrzymania całości iloczynu tych ideałów. W niniejszej pracy przedstawione zostały definicje naiwności oraz pokrewnej jej naiwności zbazowanej, podstawowe lematy ich dotyczące, przykłady wyliczone w różnych pierścieniach, wnioski wynikające z prób rozwiązania problemu, obiecujące metody, a także powiązane problemy. Każda sekcja zawiera również komentarz wyjaśniający jej sens i inne niemierzalne rezultaty pracy nad problemem naiwności.

Contents

1 Introduction

This section contains a summary of this thesis. I recommend reading this entire thesis in linear order, except when briefly following references—it should be logically ordered, to the best of my ability. In the electronic version, the references (or at least their numeral parts) are clickable.

Section 2 starts by listing basic notational and naming conventions in order to avoid possible confusion. It then presents the basic definitions used in this thesis—those of naive product, naivety and based naivety. Those definitions are given thorough explanations of their technical and intuitive meaning, as well as reasons for their existence. In the second subsection, three similar problems are briefly described in order to further embed this thesis in the existing mathematical environment.

Section 3 contains basic observations and lemmas regarding naivety and based naivety. Many of them require only single-line proofs, but they are nonetheless useful, especially when calculating the examples in the next section. All of them are the result of my work

Section 4 contains the aforementioned examples that I managed to calculate. Each example is given a proof and notes that explain its significance. Two of them borrow parts of their proofs from other works. The second subsection contains my general thoughts on calculating naivety, resulting from attempts both successful and not. A large part of this subsection is devoted to attempts using simple computer programs, including the description of the program I used to calculate or verify several of the examples.

Section 5 contains the most promising ideas on how to approach naivety. Many of them are not precisely formulated lemmas or conjectures, but rather specific perspectives which could yield results if studied in depth. Each has its own problems, but also potential benefits. I tried to write down as much of the intuition I developed over those last two years as possible.

Finally, section 6 contains a short conclusion of the thesis, summarizing the possible directions in which the work could continue.

2 Preliminaries

2.1 Definitions

2.1.1 Conventions

Throughout this article, we will assume that R is a ring (commutative, with unity), and A, B are ideals in R—subsets closed under addition and absorptive (closed under multiplication by any element of R). Elements of A and B will usually be denoted by, respectively, a and b (with appropriate indices). The (ideal) product of A and B—defined as the set of finite sums of all elements of the form ab—will be denoted by AB. Elements of AB will usually be denoted by c, and other lowercase letters will generally denote elements of R. Most ideals will be described by their generators: $(a_1, \ldots, a_n)$ denotes the set of all (finite) "linear" combinations of $a_1, \ldots, a_n$ over R (i.e. combinations of the form $r_1 a_1 + \cdots + r_n a_n$). A sum with zero summands will be considered to equal 0. For a set $X \subseteq R$, $X + X$ will denote the sum set $\{x + y : x, y \in X\}$, and rX will denote $\{ax : x \in X\}$.

We do not impose any special conditions on the rings. One could expect we would prefer to work only in integral domains (rings without zero divisors), but that assumption does not appear to be particularly helpful. Due to lemma 8, working with Noetherian rings appears to be appropriate (and in fact most examples will be such), but it is not necessary for any of the definitions to be well-founded—although infinite values appear more often in non-Noetherian rings. We will simply assume the ideals are finitely generated on a case-by-case basis.

Commutativity does not appear to be particularly vital either, but assuming it will save us from restating certain lemmas twice and wondering whether each used property of ideals depends on it or not.

2.1.2 Naive product

We define the *naive product* of A and B as $A \circ B = \{ab : a \in A, b \in B\}$, i.e. simply the set of products of elements of A and B. Finite sums of elements of this set form AB. The special name and notation is introduced in order to avoid confusion with the (ring-theoretic) ideal product, as well as to highlight its role as the "seed" of the whole ideal product. Note that $A \circ B$ always contains 0, and hence sums of length exactly n and of length up to n are the same.

2.1.3 Naivety

We define the *naivety* of A and B—the central subject of this article—as the smallest natural number n such that sums of n elements of $A \circ B$ form the entire AB. It may also equal $\omega = \aleph_0$ if the length cannot be bounded. In other words, it is the smallest sum length required to build AB from $A \circ B$. Symbolically:

$$\mathcal{N}(A, B) = \min_{n \in \mathbb{N}} \left\{ n : \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A,\, b_i \in B \right\} = AB \right\}.$$

This is not a particularly well-motivated definition. Upon learning about the ideal product, I simply asked about the required length of the sums, and it turned out to be unknown (at least as far as I was able to determine). However, it may be useful if a need arises to calculate some ideal product directly, as it provides a much simpler stop condition that checking additive closure.

We define a *representation* (with respect to A and B) of an element c as any sum of elements of $A \circ B$ that equals c. Note that it may contain zeros. A *minimal* representation will be one that has the smallest length possible (which is a stronger condition than not containing any zeros). Of course a minimal representation is rarely unique.

We may talk about the naivety of a single element c of AB—the length of the shortest representation of c. We denote it by $\mathcal{N}_{A,B}(c)$, omitting the comma when the separation of the index into two ideals is clear. We take $\mathcal{N}_{AB}(0) = 0$, as 0 is represented by the sum with zero elements. Then the naivety of A and B is the supremum of individual naiveties of each element of AB. This simple formulation is helpful when considering the observations and lemmas in the next section and highlights the fact that occasionally $\mathcal{N}(A, B) = \omega$.

We may informally say "the naivety of AB" or "the naivety of c over AB"—this is technically wrong, since naivety requires two separate ideals, and not just the resulting product. The simplest way to see this is to take any example with $\mathcal{N}(A, B) > 1$—even example 1—and note that obviously $\mathcal{N}(AB, (1)) = 1$ (see observation 9; (1) is the principal ideal generated by 1, or the whole ring). As a result, saying "the naivety of C" would be ambiguous, but the natural way of saying or writing AB as a product instead of a pair still presents both ideals, so it can be used.

Note that even though $A \circ B$ is defined using multiplication, and naivety pertains to a product of ideals, the problem itself is primarily an additive one. The naive product is already an absorptive set (closed under multiplication by any element of R), and this quality is generally hard to break, so all studied sets will retain it. As a result, it is the additive properties that will be the issue. Moreover, one could easily generalize naivety by replacing $A \circ B$ with some more general set in any abelian group, completely removing any mentions of multiplication.

The inspiration for the name "naivety" comes from [1] (p. 419), where the author states that we would (naively) like to define AB as $A \circ B$. I have also considered alternative names: "additive complexity"—as the naivety of a product determines how complicated it is in terms of certain sums, "naive rank"—to mirror terms such as tensor rank or slice rank, or "strata number"—the explanation for this one is given in 5.1. The name "naivety" has one small flaw: we would expect the *most* naive products to be the simplest ones—but instead low naivety means that the product is additively uncomplicated. Similarly, the term "naive" is used to mean low naivety (e.g. the naive product is the set of elements of naivety 1). However, since "naivety" does not yet have an established mathematical meaning, I hope this minor confusion will be easy to get over.

2.1.4 Based naivety

Note that we may rewrite the definition of naivety as:

$$\mathcal{N}(A,B) \leq n \iff (\forall c \in AB)\,(\exists a_1,\ldots,a_n)\,(\exists b_1,\ldots,b_n)\,(c = a_1b_1 + \cdots + a_nb_n)\,.$$

We define *based naivety* with a simple quantifier switch:

$$\mathcal{N}^B(A,B) \leq n \iff (\exists b_1,\ldots,b_n)\,(\forall c \in AB)\,(\exists a_1,\ldots,a_n)\,(c = a_1b_1 + \cdots + a_nb_n)\,.$$

Instead of picking a representation for each element of AB, based naivety tries to pick a *naive basis* (or basis for short) with n elements from B first, and then produce each element by multiplying the basis elements by coefficients from A. Similarly to regular naivety, it can also be infinite when a finite basis cannot be chosen.

This definition was motivated by example 5 (and the story is detailed there).

One could be tempted to define the based naivety of a particular element, as we did with regular naivety above, but it would obviously be dependent on the particular choice of basis, making such a definition notationally cumbersome at best. As of now, there seems to be little reason for considering it.

Note that—unlike regular naivety—the definition of based naivety is not symmetric. The choice to use "right based naivety" in this thesis is entirely arbitrary, and in most examples it will actually be the same from both sides. Note also that we do not require the basis to generate the entire B (but the entirety of AB must still be created from combinations over A of its elements).

Even though the definition of based naivety is secondary to that of naivety, I still believe it is worth considering. Most lemmas work just as well with based naivety as with regular naivety, and it is usually easier to calculate, so it does not require much additional work to include, while potentially providing certain bounds on naivety (described in 5.5), as well as being interesting in its own right. The relationship between naivety and based naivety can sometimes be quite intriguing as well.

The original name for based naivety was "represented naivety", and instead of basis I used "representatives". However, this caused confusion with other terms (most notably representation of an element), although it had the benefit of ease of referring to the basis elements individually. I also considered "delegated naivety", as it avoids the confusion, but stresses the interpretation that we choose representatives/delegates (as in representative democracy) who will be appointed to take care of representing elements of AB. Another option was "exhibited naivety", demonstrating the interpretation that based naivety is "clearly visible", as we do not need to search for the representations too much. Finally, I also considered "static naivety", referring to the fact that the factors from B are "statically" chosen and do not change. Ultimately, "based naivety" gets the point across well enough, and since we will rarely use any other meaning of "basis", it should not be confusing.

2.2 Related problems

While trying to determine whether naivety is an open problem, and later when attempting to seek out possible methods to apply to it, I have been referred to a few similar-sounding problems. While none of them are direct generalizations nor specializations, the definitions are similar enough to warrant a deeper investigation. I am not aware of an analogue of based naivety for any of these problems, although for strength, it could be defined in a directly analogous way (certain ideas for the other two are mentioned in 5.6).

2.2.1 Tensor rank

The first and best-known problem is the tensor rank (see [5]). A simple tensor (or tensor of rank one) is a tensor that can be written in the form $a_1 \otimes a_2 \otimes \cdots \otimes a_n$. We define the rank of a tensor A (not to be confused with its order n) as the minimum number of tensors of rank one that sum to A. The parallel between this definition and that of naivety is clear, although naivety as defined above is analogous only to the case of tensors of order 2. Section 5.6 discusses a concept similar to "increasing the order", but it seems likely that many methods usable for tensor rank could be too general (and hence too weak) for (standard) naivety, since they include higher orders.

Another issue is that tensor rank is not yet well-understood. Calculating it is generally NP-hard ([6]), and there does not seem to be many strong bounds. Nonetheless, due to this problem's relative popularity and importance, researching possible connections and attempting to copy methods may yield some results. Moreover, this problem is directly related to the computational complexity of matrix multiplication, which may turn out to be useful for naivety (see example 9 and section 5.4).

2.2.2 Slice rank

A slice is defined as any function in many variables that is of the form

$$f(x_1, \ldots, x_n) = f_1(x_i) \cdot f_2(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \qquad (\text{for any } i \in (1, \ldots, n)).$$

Intuitively speaking, it is a sort of "separable" function, one that can be described as a simple modification of a function in less variables. Predictably, the slice rank of a function g is defined as the lowest number of slices that sum to g. Usually, it is defined and studied in the context of tensors.

Slice rank has a definition that is also obviously similar to the definition of naivety. However, from our perspective, it has a similar problem to tensor rank—naivety corresponds to the simplest case of order 2, which may again result in typical methods being too general. Moreover, in the case of slice rank, the fact that we can choose any of the variables appears to be rather fundamental, and that aspect is completely lost in the case of order 2. Again, a possible rectification of this problem is discussed in 5.6.

Slice rank is also a far newer concept, introduced only in 2016 ([3]). This means that it may not yet have an abundance of methods we could attempt to appropriate for naivety, but also that if any results on naivety could be adapted for slice rank, they could more likely be novel. Moreover, slice rank is of interest due to the applications in combinatorial problems, so even if its methods do not turn out to be useful for naivety, it may turn out to be a useful tool in additive combinatorics by itself.

2.2.3 Strength of polynomials

The strength of a homogeneous polynomial (in many variables) is the most directly similar to naivety. It is defined as the length of the shortest representation $p = f_1 g_1 + \cdots + f_k g_k$, where f_i, g_i are homogeneous polynomials of degree 1. The definition looks the most alike due to using basic two-factor products (although technically it could be defined using products of more polynomials as well). Nonetheless, it still has a problem similar to choosing the excluded variable when defining a slice: this time we can choose the degree of each f_i (which forces the degree of g_i). This means that it translates relatively well into naivety, but not entirely directly: in a polynomial ring $K[x_1, \ldots, x_n]$ let $I = (x_1, \ldots, x_n)$ be the ideal generated by all monomials of degree 1. Then for a homogeneous polynomial p of degree d, we have

$$\operatorname{str}(p) \leqslant \min_{k+l=d} \mathcal{N}_{I^k, I^l}(p).$$

The proof of this fact is straightforward: each naivety-representation of p over I^k, I^l is also a strength-representation, since if any of the used elements of I^k had any terms of degree higher than k, they would ultimately need to cancel out (as p is homogeneous of degree $k + l$), so they may as well be skipped altogether. Due to the aforementioned possibility of choosing a different degree for each f_i, this inequality is not likely to become an equality (unless $d = 2$, as seen in example 9), but it is nonetheless the only (somewhat) closed-form relation between naivety and some preexisting problem that we have. Moreover, a lot of the simplest examples use (potentially modified) polynomial rings, which may mean that both the strength itself and methods used for it may be applicable. And conversely, results on naivety could provide rather strong upper bounds on strength (since the minimum over a few different pairs of ideals may be quite low even if the individual bounds are not great on average).

The subject of strength of polynomials is also a relatively new one. It is nicely described in [2], from whence we took a part of the proof of example 9. The fact that two similar terms (tensor rank and strength) have been introduced recently is rather optimistic for naivety—both suggesting that it may be a novel question, and embedding it in a new, dynamic current.

3 Basic properties

This section contains various lemmas and observations that can provide bounds on naivety and based naivety. One important thing to note about them is that while we can often get relatively tight upper bounds—either from these lemmas, or by finding a basis—finding a good lower bound is quite problematic, and usually requires finding an element with high naivety.

Even though in most cases bounds on both naivety and based naivety are provided, the latter is usually an afterthought, added simply because it did not create much additional effort. The same is true for the examples in the next section. Nonetheless, future results could potentially show that bounds on based naivety are as important as those on regular naivety (see 5.5).

For simplicity, this section assumes the reader is acquaintanced with the simple interpretation that the naivety of A and B is the supremum of individual naiveties of all elements of AB.

3.1 Simple observations

Observation 1. If AB contains an irreducible element and both A and B are proper ideals, then $\mathcal{N}(A, B) > 1$.

Obviously an irreducible element cannot be represented by a sum of length 1, i.e. a product.

This observation will commonly be used in examples to provide a lower bound of 2 on naivety and based naivety.

Observation 2. Sums of elements of $A \circ B$ shorter than $\mathcal{N}(A, B)$ cannot give an ideal.

We already have absorptivity, but not closure under addition. If the set $(AB)_l$ of all sums up to length $l < \mathcal{N}(A, B)$ was closed under addition, then adding elements of $A \circ B$ would not create anything new (as elements of $A \circ B$ are those with naivety 1, and hence are contained in $(AB)_l$), and it would mean that $(AB)_l = AB$ and $\mathcal{N}(A, B) = l$.

Observation 3. Naivety of elements is subadditive.

If

$$c^{(1)} = a_1^{(1)} b_1^{(1)} + \cdots + a_k^{(1)} b_k^{(1)}$$

and

$$c^{(2)} = a_1^{(2)} b_1^{(2)} + \cdots + a_l^{(2)} b_l^{(2)},$$

then

$$c^{(1)} + c^{(2)} = a_1^{(1)} b_1^{(1)} + \cdots + a_k^{(1)} b_k^{(1)} + a_1^{(2)} b_1^{(2)} + \cdots + a_l^{(2)} b_l^{(2)}.$$

Obviously the naivety of $c^{(1)} + c^{(2)}$ will usually end up much smaller than $k + l$, since there may be other representations. In particular, $k + l$ may be greater than $\mathcal{N}(A, B)$.

Observation 4. Naivety of elements does not increase with multiplication.

If $c = a_1 b_1 + \cdots + a_k b_k$, then $rc = ra_1 b_1 + \cdots + ra_k b_k$, and since A is an ideal, and hence absorbtive, $ra_i \in A$ (we could also absorb the r into B). This is a direct result of $A \circ B$ (as well as other sets, such as the results of sums up to a particular length) being absorptive, and shows that multiplication is rarely an issue. Of course we may have $\mathcal{N}_{AB}(rc) < \mathcal{N}_{AB}(c)$—take for instance example 2 ($R = \mathbb{Z}[\sqrt{-5}]$, $A = (2, 1 + \sqrt{-5})$, $B = (2, 1 - \sqrt{-5})$), where $\mathcal{N}_{AB}(4) = 1$, since $4 = 2 \cdot 2$ and $2 \in A, 2 \in B$, but $\mathcal{N}_{AB}(2) = 2$ (since 2 is irreducible, see the example's proof).

Observation 5. Naivety of an element does not increase when we send the element through a homomorphism. In other words, when passing from R to R/I, $\mathcal{N}(A,B) \geqslant \mathcal{N}(A/I, B/I)$. The same is true for based naivety.

If f is a homomorphism and $c = a_1b_1 + \cdots + a_kb_k$, then $f(c) = f(a_1)f(b_1) + \cdots + f(a_k)f(b_k)$. If $(b_1, \ldots, b_k)$ is a valid basis, then so is $(f(b_1), \ldots, f(b_k))$.

Quotient rings can be very convenient for creating examples. Often, it is useful to think in the other direction: the naivety in a quotient ring gives a lower bound for naivety in the original ring.

Observation 6. Nased naivety is never smaller than regular naivety.

Regardless of the choice of basis $(b_1, \ldots, b_k)$, $c = a_1b_1 + \cdots + a_kb_k$ is also a perfectly valid representation of c. This is not a particularly surprising observation, given that the definition of based naivety is directly harder to satisfy than that of naivety.

Observation 7. If $R = R_1 \times R_2, A = A_1 \times A_2, B = B_1 \times B_2$, then
$\mathcal{N}(A,B) = \max\{\mathcal{N}(A_1,B_1), \mathcal{N}(A_2,B_2)\}$ and $\mathcal{N}^B(A,B) = \max\left\{\mathcal{N}^B(A_1,B_1), \mathcal{N}^B(A_2,B_2)\right\}$.

This observation is a direct consequence of the fact that in a Cartesian product, the first and second coordinate are entirely independent. This means that we must find a representation for both coordinates of an element of AB separately, then combine them in any way we choose (potentially adding zeros to the shorter one), and we obviously may not get a shorter representation than either of the constituent representations. The same logic applies to based naivety, as we need to choose a basis on each coordinate separately.

Note that if $R = R_1 \times R_2$, then every ideal is of the form $I = I_1 \times I_2$. This follows from absorptivity: we may multiply an ideal by $(1,0)$ or $(0,1)$ to show that each ideal contains its projections on both axes, and since it is closed under addition, it also contains any combination of values on each coordinate.

This observation remains true if R is a product of more than two rings. It also remains true if we replace the Cartesian product with an infinite direct sum, with the proof practically unchanged (the Cartesian product and direct sum of rings are the same in the finite case). An infinite Cartesian product of rings may have "elements with infinite naivety" (if they have increasing naiveties of each coordinate), but the observation remains valid if we replace the maximum with supremum.

This observation is quite useless for creating interesting examples—it can only be used to show that an example can be reduced to a set of simpler ones. Its only clear use lies in building big ugly examples with infinite naivety (although the only big ugly one included in this thesis—example 12—uses a different technique).

3.2 Basic lemmas

Lemma 8. (The generator bound) Let B be finitely generated, $B = (b_1, \ldots, b_k)$. Then $\mathcal{N}(A, B) \leqslant k$ and $\mathcal{N}^B(A, B) \leqslant k$. The bound on naivety also holds if $A = (a_1, \ldots, a_k)$.

The proof is not complicated: note that if $c = \alpha_1\beta_1 + \cdots + \alpha_l\beta_l$ ($\alpha_i \in A, \beta_i \in B, c \in AB$), for each β_i we have $\beta_i = r_1^{(i)}b_1 + \cdots + r_k^{(i)}b_k$, and thus we can reorganize the entire representation into

$$c = (r_1^{(1)}\alpha_1 + r_1^{(2)}\alpha_2 + \cdots + r_1^{(l)}\alpha_l)b_1 + \cdots + (r_k^{(1)}\alpha_1 + r_k^{(2)}\alpha_2 + \cdots + r_k^{(l)}\alpha_l)b_k$$

and thus $\mathcal{N}_{AB}(c) \leqslant k$ for each $c \in AB$. Of course we may also do the same with the roles of A and B reversed.

Alternatively, one could simply note that $(b_1, \ldots, b_k)$ is a valid basis, thus giving the bound on based naivety, and through observation 6, also on regular naivety.

Despite its simplicity, this is probably the most important statement in this entire thesis. Since in most cases the considered ideals are quite simple—which often means they have relatively few generators—the bounds are quite tight. Moreover, since ideals are most commonly described using generators, this lemma is often easily applicable. However, despite having so few possible values, naivety remains difficult to calculate precisely.

Observation 9. If A or B is a principal ideal (i.e. is generated by one element), then $\mathcal{N}(A, B) = 1$. If B specifically is principal, then also $\mathcal{N}^B(A, B) = 1$.

This is a direct result of the generator bound. In particular, this means that principal ideal domains are of no interest to us (that includes euclidean rings and fields). There are also principal ideal rings that are not integral domains, but those are similarly boring for us.

Lemma 10. Let AB be finitely generated, $AB = (c_1, \ldots, c_n)$. Then $\mathcal{N}(A, B) \leqslant \sum_{i=1}^{n} \mathcal{N}_{AB}(c_i)$ and $\mathcal{N}^B(A, B) \leqslant \sum_{i=1}^{n} \mathcal{N}_{AB}(c_i)$.

The proof is mostly analogous to that of the generator bound: let $k_i = \mathcal{N}_{AB}(c_i)$. For any c in AB, we have $c = r_1c_1 + \cdots + r_kc_k$. For each i we can write

$$r_ic_i = r_ia_1^{(i)}b_1^{(i)} + \cdots + r_ia_{k_i}^{(i)}b_{k_i}^{(i)}$$

and sum these to get a representation of c of the specified length. We also have a basis $\left\{b_k^{(i)} : i \in (1, \ldots, n), k \in (1, \ldots, k_i)\right\}$ of the specified size—since an appropriate part of it (corresponding to the given i) can produce each c_i, it can produce any element of AB.

This is a sort of symmetric lemma to the generator bound, although not nearly as useful. It usually does not provide similarly tight bounds (since each generator can be "worth" more than 1), but is can be useful in cases where AB luckily ends up with fewer generators than either A or B (such as observation 11 below). However, using this lemma effectively requires finding a *good* set of generators, which may not be trivial.

Observation 11. If $AB = (c)$ is principal, then $\mathcal{N}(A, B) = \mathcal{N}^B(A, B) = \mathcal{N}_{AB}(c)$.

This is a direct result of lemma 10 (since we obviously cannot have $\mathcal{N}(A, B) \leq \mathcal{N}_{AB}(c)$). It allows us to shorten our calculations when AB happens to be principal (which is not particularly uncommon in Noetherian rings).

Lemma 12. In an integral domain, if A_1, A_2 are in the same class, and B_1, B_2 are in the same class, then $\mathcal{N}(A_1, B_1) = \mathcal{N}(A_2, B_2)$ and $\mathcal{N}^B(A_1, B_1) = \mathcal{N}^B(A_2, B_2)$.

In an integral domain R, we say that ideals I, J are in the same class, if there are $r, s \in R \setminus \{0\}$ such that $rI = sJ$. In certain types of rings (e.g. algebraic integer rings), the number of such classes is an extensively studied question.

The proof of the lemma follows from the fact that multiplication in an integral domain is cancellable, i.e. $ab = ac \implies b = c$. Let $r_1A_1 = r_2A_2 = A$ and $s_1B_1 = s_2B_2 = B$ ($r_1, r_2, s_1, s_2 \in R \setminus \{0\}$). We will show that $\mathcal{N}(A_1, B_1) = \mathcal{N}(A, B)$ (and the proof for A_2, B_2 is entirely analogous).

It is clear that $\mathcal{N}(A_1, B_1) \geqslant \mathcal{N}(A, B)$—one may simply multiply each representation over A_1, B_1 by r_1s_1 to get a representation (of the same length) over A, B, and this provides representations for all elements, because $AB = r_1s_1A_1B_1$, i.e. each element of AB is of the form r_1s_1c for $c \in A_1B_1$.

Now assume that $\mathcal{N}(A, B) = n$. Then there is a $c \in A_1B_1$ such that $\mathcal{N}_{AB}(r_1s_1c) = n$ or $r_1s_1c = r_1a_1s_1b_1 + \cdots + r_1a_ns_1b_n$ ($a_i \in A_1, b_i \in B_1$)—again because $AB = r_1s_1A_1B_1$. Then the cancellation property implies that $c = a_1b_1 + \cdots + a_nb_n$. But since c was an arbitrary element of A_1B_1, that means that $\mathcal{N}(A_1, B_1) \leqslant k$.

The proof for based naivety is analogous: we have $\mathcal{N}^B(A_1, B_1) \geqslant \mathcal{N}^B(A, B)$, since any basis of A_1, B_1 can be multiplied by s_1 to get a basis of A, B. If we had a smaller basis of A, B, we could similarly use the cancellation property to get a basis of the same size of A_1, B_1 (along with representations of every element, proving that it is valid).

This proof is effectively just an application of the fact that multiplication by a given non-zero element in an integral domain is a module isomorphism (of the above ideals).

This lemma is of particular use in the aforementioned algebraic integer rings, as their class numbers are known in many cases, and are generally low (and always finite). This means that we can gain complete knowledge of naivety in the entire ring by checking just a few cases—especially that by observation 9, any case involving the class of principal ideals is trivial.

4 Examples and computations

4.1 Examples

This section contains the examples I have managed to compute while studying the problem. Each example will be presented by listing the ring it takes place in, the ideals A and B, and the resulting naivety and based naivety. A proof and notes detailing the significance and important conclusions of the given example will follow. Certain examples will also depend on a parameter—in that case, it is understood that the example remains true for any value of it.

In most cases, the upper bound on based naivety will simply be provided by explicitly showing a basis (and a proof that any element of AB can be represented as a "linear" combination of its elements). The lower bound will be attained by various means, depending on the particular example.

Example 1. $R = \mathbb{Z}[x]$ (polynomials over integers)
$A = (x, 2)$ (polynomials with an even constant term)
$B = (x, 5)$ (polynomials with a constant term divisible by 5)
$AB = (x, 10)$ (polynomials with a constant term divisible by 10)
$\mathcal{N}(A, B) = 2, \quad \mathcal{N}^B(A, B) = 2$

Proof: Since $2x$ and $5x$ are obviously in AB, then so is their combination x. Obviously $10 = 2 \cdot 5$ is in AB as well, and any element of AB clearly has a constant term divisible by 10. This proves that $AB = (x, 10)$.

The generator bound limits naivety and based naivety by 2, since B has two generators. Then, $x^2 + 10 = (x \cdot x) + (2 \cdot 5)$ is an irreducible element in AB, so by observation 1 neither naivety nor based naivety can be 1. Since the upper and lower bounds are equal, we have successfully calculated both naivety and based naivety.

Notes: This is an extremely simple example, proving that at least sometimes we do not have $AB = A \circ B$, and hence the problem of naivety is not trivial.

Example 2. $R = \mathbb{Z}[\sqrt{-5}]$ (the ring of algebraic integers in $\mathbb{Q}(\sqrt{-5})$)
$A = (2, 1 + \sqrt{-5})$
$B = (2, 1 - \sqrt{-5})$ (the complex conjugate of A)
$AB = (2)$
$\mathcal{N}(A, B) = 2, \quad \mathcal{N}^B(A, B) = 2$

Proof: In algebraic integer rings such as R, we can define a multiplicative norm, which is 1 only on units (see [1], p. 414). In R, an element $a + b\sqrt{-5}$ has norm $a^2 + 5b^2$.

The generator bound limits naivety and based naivety to 2, and 2 is an irreducible element in AB—it has norm 4, and there are no elements with norm 2 (the equation $a^2 + 5b^2 = 2$ has no integer solutions), but the norm is multiplicative.

Notes: This example was taken from [1] (p. 420), which means that it is the most verified of all examples. The fact that algebraic integer rings have such a norm appears to be quite powerful, but I have not yet managed to use it for anything better than invoking observations 1 and 11.

Since R has ideal class number 2 ([1], p. 431), it only has two classes of ideals—principal and non-principal. Since by observation 9 any product involving a principal ideal has naivety one, we have now determined the naivety of any pair of ideals in the entire ring (by lemma 12).

Example 3. $R = \mathbb{Z}[x^{\mathbb{R}_{0+}}]$ (the ring of "polynomials with nonnegative real exponents" over $\mathbb{Z}$, or the combinations over $\mathbb{Z}$ of all nonnegative powers of x)
$A = B = (x, x^{1/2}, x^{1/3}, x^{1/4}, \dots)$ (the ideal of all elements without a free term)
$A^2 = A$
$\mathcal{N}(A, A) = 1, \quad \mathcal{N}^B(A, A) = \omega$

Proof: Each element c of $AB = A$ can be represented as a product of x raised to a power smaller than the smallest power appearing in c and an appropriate second factor.

We cannot have a finite basis, since then we could pick an exponent lower that the lowest in all of them, and we could not represent it—but $(x, x^{1/2}, x^{1/3}, x^{1/4}, \dots)$ is a countable basis.

Notes: This is an example of naivety equaling one, even though neither of the ideals is principal (if A was principal, we could take x raised to a power smaller than the smallest exponent in the generator, which is a contradiction). However, the ring is obviously not Noetherian (in fact, A is not finitely generated).

Example 4. $R = \mathbb{Z}[x]$
$A = B = (x^n, 2x^{n-1}, 4x^{n-2}, \dots, 2^n)$
$A^2 = (x^{2n}, 2x^{2n-1}, 4x^{2n-2}, \dots, 2^{2n})$
$\mathcal{N}(A, A) = 2, \quad \mathcal{N}^B(A, A) = 2$

Proof: The basis is $(x^n, 2^n)$—the first n generators of A^2 are divisible by x^n, and the last n by 2^n, and the required coefficients (for any combination of these generators) are easily verified to be in A. By Perron's irreducibility criterion we know that $x^{2n} + 2^{2n+1}x^{2n-1} + 2^{2n}$ is an irreducible element in AB.

Notes: Since A cannot be generated by less than $n + 1$ generators (since each new power of x requires more precision than the previous one), this example shows that naivety (and based naivety) can remain small even if the ideals have a lot of generators.

Note also that the elements of the basis have a slight "overlap", as the middle term is a multiple of $2^n x^n$. This may suggest that perhaps based naivety is actually "slightly smaller than 2" in some complicated sense (which could mean, for instance, that we may worsen this example slightly and still have $\mathcal{N}^B = 2$).

Example 5. $R = \mathbb{Z}[x]/(x^{n+1})$
$A = B = (x^n, 2x^{n-1}, 4x^{n-2}, \ldots, 2^n)$
$A^2 = (2^n x^n, 2^{n+1}x^{n-1}, 2^{n+2}x^{n-2}, \ldots, 2^{2n})$
$\mathcal{N}(A, A) = 1, \quad \mathcal{N}^B(A, A) = 1$

Proof: The basis needs only a single element: 2^n, as all terms of each element of A^2 are divisible by it (and the other factor is again easily verified to be in A).

Notes: This is a simple modification of the previous example. We could also use the similar modification $\mathbb{Z}[x]/(x^n)$ (which is a quotient ring of the current R). Doing so would clearly present the natural behavior that setting one element of the basis to equal zero has reduced the based naivety by 1 (as compared to taking it in $\mathbb{Z}[x]$). However, we still have $\mathcal{N}^B = 1$ even with the slightly bigger ring $\mathbb{Z}[x]/(x^{n+1})$ (but not with $\mathbb{Z}[x]/(x^{n+2})$), which may or may not be related to the previous example's based naivety being "slightly smaller than 2".

This is also (almost) the example that motivated based naivety. For $n = 2$ and taken modulo 16, it is finite and small enough to be calculated by brute force on a blackboard. While searching for the decomposition (over A, B) of each of the 8 elements of AB, I noticed that they were all divisible by 4, which is an element of A. Gradual expansion of the example into example 4 and then example 7 has shown the usefulness of starting by trying to find a basis and led to the birth of based naivety, as well as some strong conjectures detailed in further sections.

Example 6. $R = \mathbb{Z}[x]/(210, x^3)$
$A = (x^2, 7x, 14)$
$B = (x^2, 5x, 15)$
$AB = (x^2, 35x)$
$\mathcal{N}(A, B) = 1, \quad \mathcal{N}^B(A, B) = 1$

Proof: Note that $15 \cdot x^2 \in AB$ and $x^2 \cdot 14 \in AB$, and so their difference x^2 is also in AB. Similarly we get $35x \in AB$, and the linear terms of all elements of AB are divisible by 35 (and we may easily get any multiple of 35). All free terms of elements of AB are multiples of $15 \cdot 14 = 210$, and hence equal 0 in R, which shows that $AB = (x^2, 35x)$.

The single basis element is $x^2 + 5x + 15$. Let $ax^2 + 35bx \in AB$. We need to find $d, e, f \in \mathbb{Z}_{210}$ such that $(dx^2 + 7ex + 14f)(x^2 + 5x + 15) = ax^2 + 35bx$. We may rewrite that as:

$$\begin{cases} b = 2f + 3e \\ a = 14f + 35e + 15d \end{cases}$$

or, equivalently

$$\begin{cases} 2f = b - 3e \\ a = 7b + 14e + 15d. \end{cases}$$

So we only need to find d, e such that $15d + 14e = a - 7b$ and e has the same parity as b (since we need to divide $b - 3e$ by 2 to get f). But since 14 and 15 are coprime, fulfilling the first condition is always possible, and we can fulfill the second by adding 14 to d and subtracting 15 from e.

Notes: This modifies example 7 in a very similar fashion to example 5 modifying example 4 (I apologize for the awkward ordering, but it could not be avoided). Note that this makes the example finite (and so does a quotient with an exponent higher than 3, which seems to keep $\mathcal{N} = 2$), so it could be verified by a computer. Originally the ideals were $(x^2, 2x, 6)$ and $(x^2, 5x, 35)$, but the current ordering of the prime factors has the smallest amount of calculations (least cardinality of A and B) while not being meaningfully different.

Example 7. $R = \mathbb{Z}[x]/(210)$
$A = (x^2, 7x, 14)$
$B = (x^2, 5x, 15)$
$AB = (x^2, 35x)$
$\mathcal{N}(A, B) = 2, \quad \mathcal{N}^B(A, B) = 2$

Proof: The proof that $AB = (x^2, 35x)$ can be copied from example 6. The element $x^2 + 35x$ does not reduce into a product of the form ab with $a \in A, b \in B$ (which is a finite check, since the degrees of a and b are bounded by 2), so $\mathcal{N}(A, B) > 1$. The basis has two elements: $x^2 + 5x + 15$ and x^2. We will now prove that it is valid (by expressing any element of AB using this basis).

We know from example 6 that $x^2 + 5x + 15$ can be used to set the linear and quadratic terms to whatever we need (with a suitably chosen coefficient $\alpha_1 \in A$ of degree $\leqslant 2$). Note that if we added a new term cx^3 to α_1, it would not change those two terms, but would change the cubic term of the result by $15c$. So, for any element of AB, we first set the linear and quadratic terms, as well as the cubic term modulo 14 ($= 210/15$) to whatever we need by manipulating α_1, and then adjust the coefficient α_2 for x^2 to set the cubic term modulo 15 and all higher terms to whatever we need without breaking the other coefficients (α_2 does not have a constant term; its linear term is divisible by 7, so we can change the resulting cubic coefficient by 14 easily).

Notes: This is effectively a variant of example 4, modified to have $A \neq B$ and generally be a bit more complicated. It could most likely be expanded in a similar fashion by using more primes, although adapting the same proof would likely be extremely tedious. The quotient by 210 appears necessary to keep naivety lower than 3.

Both here and in example 4 the basis is built from the generators of B in a very simple fashion, which may suggest that looking at "simple" combinations of generators is a way to find the basis in general.

Example 8. $R = \mathbb{C}[x_1, \ldots, x_k, y_1, \ldots, y_l]/((x_i x_j | i, j \in \{1, .., k\}) + (y_i y_j | i, j \in \{1, \ldots, l\}) + I^3)$ (where I^3 is the ideal generated by all monomials of degree 3; we want to only consider monomials of the form xy in AB)
$A = (x_1, \ldots, x_k)$
$B = (y_1, \ldots, y_l)$
$AB = (x_i y_j | i \in \{1, .., k\}, j \in \{1, \ldots, l\})$
$\mathcal{N}(A, B) \leqslant \min\{k, l\}, \quad \mathcal{N}^B(A, B) = l, \quad \mathcal{N}^B(B, A) = k$

Proof: Naivety is limited by the generator bound (and finding a lower bound is both difficult and not important for the purposes of this example). Both based naiveties are similarly bounded by the generator bound, but proving the lower bound is the important part.

Note that we may consider elements of A and B to only contain monomials of degree 1—any monomials of higher degree vanish after multiplication by an element of the other ideal. Assume we could choose a basis with less than l elements from B—$(b_1, \ldots, b_m)$. Then, since B (with the above restriction) is also a vector space over $\mathbb{C}$ of dimension l, we could find an invertible linear transformation F which would send $b_1, \ldots, b_m$ to, respectively, $y_1, \ldots, y_m$. But such a linear transformation induces a ring isomorphism. This means that since now any element with y_l cannot be represented, the pre-image of these elements could not be represented by the original basis.

Notes: This example serves two functions: it shows that based naivety is indeed not symmetric, and it provides a proof of the lower bound on based naivety for the following examples.

Example 9. $R = \mathbb{C}[x_1, x_2, \ldots, x_n]/A^3$ (we want to ignore anything of degree 3 or higher)
$A = B = (x_1, x_2, \ldots, x_n)$
$A^2 = (x_1^2, x_2^2, \ldots, x_n^2, x_1x_2, x_1x_3, \ldots, x_2x_3, \ldots, x_{n-1}x_n)$ (the ideal generated by all monomials of degree 2, which is the ideal of all homogeneous polynomials of degree 2)
$\mathcal{N}(A, B) = \left\lceil \frac{n}{2} \right\rceil, \quad \mathcal{N}^B(A, B) = n$

Proof: The upper bound on based naivety follows from the generator bound, while the lower bound uses a very similar argument as example 8—if the basis had less than n elements, after the linear transformation, we would not be able to represent anything containing x_n^2 (since the coefficient of each element of the basis can only provide us with x_n^1—see below). Calculating naivety is a little more difficult.

We may use a restriction similar to the one in example 8. Since any monomial of degree 3 or higher equals 0 in R, we may consider A to be effectively the set of homogeneous polynomials of degree 1, while A^2 is the set of homogeneous polynomials of degree 2. This means that the naivety and strength of each element of AB are one and the same. This allows us to use the proof from [2], which I will now present:

First, we note that homogeneous polynomials of degree 2 (in n variables, over $\mathbb{C}$) are in correspondence with symmetric matrices ($n \times n$, over $\mathbb{C}$): a matrix A corresponds to the polynomial $(x_1, \ldots, x_n)A(x_1, \ldots, x_n)^\top$. This correspondence is bijective.

Recall that the rank of a matrix is equal to the smallest number of rank one matrices whose sum is the given matrix, and that rank one matrices are precisely outer products of vectors $vw^\top$ (vectors are vertical). Choose a homogeneous quadratic polynomial f. Let A be the matrix corresponding to it. Then we have the following equivalence

$$\operatorname{str}(f) \leqslant k \iff A \text{ is a sum of } k \text{ matrices of rank 2} \iff \operatorname{rnk}(A) \leqslant 2k$$

which we will now prove.

The rightward implications are relatively simple: a polynomial of stregth at most k has a representation as a sum of k products of polynomials. Each product of polynomials corresponds by the above formula to a matrix of rank at most 2 (a sum of two outer products):

$$2 \cdot (x_1, \ldots, x_n)v \cdot (x_1, \ldots, x_n)w \leftrightarrow vw^\top + wv^\top.$$

Finally, a sum of k matrices of rank at most 2 has a rank at most $2k$.

Now, assume $\operatorname{rnk}(A) \leqslant 2k$. The leftward implications use the well-known fact that a symmetric matrix A over $\mathbb{C}$ can be represented as $VDV^\top$, where D is diagonal and V is invertible. As such, we may write $D = D_1 + \cdots + D_k$, where each D_i has at most two non-zero elements: positions number $2i-1$ and $2i$ on the diagonal. That means that each D_i corresponds to a polynomial that is of the form $ax^2 + by^2$. But over $\mathbb{C}$, such a polynomial is product of two linear polynomials: $ax^2 + by^2 = (\sqrt{a}x + i\sqrt{b}y)(\sqrt{a}x - i\sqrt{b}y)$. This means that the polynomial corresponding to A can be represented as a sum of k products, each of them corresponding to a matrix $VD_iV^\top$.

I have also found a somewhat simpler restatement of this proof. Take a polynomial $p \in AB$. By Lagrange's method of completing the square, we may rewrite it as $p_1^2 + p_{2\sim}$, where $p_{2\sim}$ does not contain x_1. In Lagrange's method, we may sometimes need to substitute the variables, but that does not affect this proof. By applying this again to $p_{2\sim}$, we get $p = p_1^2 + p_2^2 + p_{3\sim}$. Continuing this process, we get $p = p_1^2 + p_2^2 + \cdots + p_n^2$, where each p_i does not contain any x_j with $j < i$. Since we are over $\mathbb{C}$, a sum of two squares is a product (just like above), and a single square is obviously a product as well, so we get $\mathcal{N}_{A,A}(p) = \left\lceil \frac{n}{2} \right\rceil$.

Notes: This example serves to both tie naivety and strength together, as well as provide certain insights on based naivety (which will be detailed in 5.5). The quotient by A^3 appears necessary to keep naivety lower than n—although I do not have a proof, it appears likely that something like $x_1^2 + x_2^3 + x_3^7 + x_4^{17}$ cannot be represented as a sum of three products only, even over $\mathbb{C}$.

Example 10. $R = \mathbb{R}[x_1, x_2, \ldots, x_n]/A^3$
$A = B = (x_1, x_2, \ldots, x_n)$
$A^2 = (x_1^2, x_2^2, \ldots, x_n^2, x_1x_2, x_1x_3, \ldots, x_2x_3, \ldots, x_{n-1}x_n)$
$\mathcal{N}(A, B) = n, \quad \mathcal{N}^B(A, B) = n$

Proof: Based naivety is calculated just like in example 9, and we only need to prove the lower bound on naivety.

We will show that $\mathcal{N}_{A,A}(x_1^2 + \cdots + x_n^2) \geqslant n$. Assume that it is lower than n and $x_1^2 + \cdots + x_n^2 = a_1b_1 + \cdots + a_{n-1}b_{n-1}$, where a_i, b_i are homogeneous polynomials of degree 1 (restriction as in example 9). This means that the set of roots of each product a_ib_i is the union of two linear subspaces of codimension 1 (those subspaces may be equal). That means that the set of roots of $a_1b_1 + a_2b_2$ is a union of some subspaces of codimension at most 2. By adding yet another product, we may only increase the codimension by at most 1, so in the end, the set of roots of the whole sum will be a union of some subspaces of *dimension* at least 1. However $x_1^2 + \cdots + x_n^2$ has only one root—$(0, 0, \ldots, 0)$—and is positive everywhere else. Thus we have reached the desired contradiction.

Notes: This example is a sort of counterpoint to example 9. Their relationship and significance will be explained in 5.5. Note that by Observation 5, the quotient by A^3 is not actually necessary.

The same proof would not work over $\mathbb{C}$—squares would not be necessarily positive and the set of roots of the left side would be bigger.

Example 11. $R = \mathbb{C}[x_1, x_2, \ldots, x_{2n}]/(A^3 + (x_i x_j | i \neq j \wedge (i,j) \notin \{(1,2),(3,4),\ldots,(2n-1,2n)\}))$
(we want to ignore all mixed terms except for $x_1x_2, x_3x_4, \ldots$ and anything of degree 3 and higher)
$A = B = (x_1, x_2, \ldots, x_{2n})$
$A^2 = (x_1^2, x_2^2, \ldots, x_{2n}^2, x_1x_2, x_3x_4, \ldots, x_{2n-1}x_{2n})$
$\mathcal{N}(A,B) = 1, \quad \mathcal{N}^B(A,B) = 2$

Proof: The basis has only two elements: $x_1 + x_2 + x_3 + x_4 + \cdots + x_{2n}$ and $x_2 + x_4 + x_6 + \cdots + x_{2n}$. To represent an element of AB, we choose the coefficient from A for the first basis element in such a way as to get appropriate coefficients next to each square (ignoring the change to coefficients of mixed terms). Then, we choose a coefficient of the form $a_1x_1 + a_3x_3 + \cdots + a_{2n-1}x_{2n-1}$ for the second one in order to get appropriate coefficients for the mixed terms without changing the coefficients next to each square.

We cannot use a basis with only one element—multiplying elements of A by it would be a linear transform, A has dimension $2n$ (over $\mathbb{C}$), but A^2 has dimension $3n$, so we would not be able to ever get the whole A^2.

The naivety is 1, since any element of A^2 can be written as

$$(\alpha_1 x_1^2 + \alpha_{1,2} x_1 x_2 + \alpha_2 x_2^2) + (\alpha_3 x_3^2 + \alpha_{3,4} x_3 x_4 + \alpha_4 x_4^2) + \cdots + (\alpha_{2n-1} x_{2n-1}^2 + \alpha_{2n-1,2n} x_{2n-1} x_{2n} + \alpha_{2n} x_{2n}^2).$$

We can write each of the terms in parentheses as a sum of two squares (by using Lagrange's completing the square, as in example 9), and hence a product $a_i b_i$. Finally, we can write the sum of these products as $(\sum a_i)(\sum b_i)$, since all mixed terms between a_i and b_j are set to zero if $i \neq j$.

Notes: This example is obviously a modification of example 9 and will be elaborated upon in 5.5. However, it has certain noteworthy qualities: it provides and example with $\mathcal{N} = 1$ where neither of the ideals is principal (and the ring is Noetherian), and even though the ring and ideals depend on a parameter n, neither the naivety nor based naivety do. It also exhibits a certain "based naivety surplus" (similarly to example 4), this time because the coefficient for the second basis element can come from a limited subset of A. This "surplus" can be utilized by reintroducing certain mixed terms—at least for $n = 2$, the term x_1x_3 can be re-added without changing the outcome.

Example 12. $R = \mathbb{C}[x_1, x_2, \dots] = \mathbb{C}[x_1] \cup \mathbb{C}[x_1, x_2] \cup \mathbb{C}[x_1, x_2, x_3] \cup \dots$
$A = B = (x_1, x_2, \dots)$
$A^2 = (x_1^2, x_2^2, \dots, x_1x_2, x_1x_3, x_2x_3 \dots)$
$\mathcal{N}(A, B) = \omega, \quad \mathcal{N}^B(A, B) = \omega$

Proof: Any minimal representation of a homogeneous $c \in AB$ of degree 2 contains a finite number of polynomials, which are in turn finite sums of monomials. This means that the representation is contained in some ring $\mathbb{C}[x_1, \dots, x_n]$. Moreover, using variables with indices higher than those appearing in c may not shorten the minimal representation of c, as we could simply set those superfluous variables to 0 and get a shorter representation. As a result, c may have naivety as high as $\lceil \frac{n}{2} \rceil$ (by example 9 and observation 5). That means that there are elements with arbitrarily high naivety. We have the obvious countable basis $(x_1, x_2, ...)$.

Notes: This example is neither aesthetically pleasing nor particularly valuable. Its purpose is simply to show that naivety may be infinite.

Example 13. $R = \mathbb{F}_p[x_1, x_2]/A^3$ (where $p \in \{3, 5, 7, 11, 13, 17, 19, 23\}$ and $\mathbb{F}_p$ is the field with p elements; we want to ignore anything of degree 3 and higher)
$A = B = (x_1, x_2)$
$A^2 = (x_1^2, x_1x_2, x_2^2)$
$\mathcal{N}(A, B) = 2, \quad \mathcal{N}^B(A, B) = 2$

Proof: The naivety in this example was proven by the computer program described in 4.2.2. Based naivety is bounded from above by the generator bound, and from below by naivety.

Notes: This example is not particularly meaningful, since the naivety is bounded by 2 anyway. With only two variables, quite high values of p can be calculated in reasonable time. The following example has more interesting behavior.

Example 14. $R = \mathbb{F}_p[x_1, x_2, x_3, x_4]/A^3$ (where $p \in \{2, 3, 4, 5\}$ and $\mathbb{F}_p$ is the field with p elements; we want to ignore anything of degree 3 and higher)
$A = B = (x_1, x_2, x_3, x_4)$
$A^2 = (x_1^2, x_2^2, \dots, x_1x_2, x_1x_3, \dots)$
$\mathcal{N}(A, B) = 3, \quad \mathcal{N}^B(A, B) = 4$

Proof: The naivety in this example was proven by the computer program described in 4.2.2. The proof that $\mathcal{N}^B(A, B) = 4$ is analogous to that in example 9.

Notes: This example is effectively a finite variant of examples 9 and 10. Due to said finiteness, we can study the sizes of $A \circ B$, $(A \circ B) + (A \circ B)$, and AB (see 5.1). Moreover, the naivety is sharply between $\mathcal{N}^B$ and $\frac{1}{2}\mathcal{N}^B$ (see 5.5). Of note is also the fact that naivety remained the same for $\mathbb{F}_4$, even though 4 is not a prime number.

The time to calculate this example was measured in hours. It is easy to see that the number of variables has the highest impact—even for $\mathbb{F}_2$, an example with 8 variables would take too long on a personal computer.

4.2 Notes on calculating naivety

As a thorough reader may have already noticed, calculating naivety is a rather annoying process—at this point, there are no general methods and each small group of examples needs to be considered separately. Even though the examples above were mostly in various types of polynomial rings, they still required separate techniques, some of them somewhat burdensome (e.g. examples 7 and 9)—and they would likely grow much more difficult if we complicated these examples even slightly. This shows that stronger theorems or techniques would be quite beneficial, should a need to calculate naivety arise. Based naivety is usually easier to calculate (but not always—see example 7, which can be calculated much faster using lemma 14, if we do not care about based naivety), since finding a basis is often simpler than proving that each element has a sufficiently short representation.

4.2.1 Computer calculations

Attempts to calculate naivety using a computer (or a particularly stubborn friend) face the fundamental issue that computers work best with finite objects, and few rings are finite. Sometimes, one can reduce the example to a finite case using quotients (see examples 5 and 6) and try to control whether the naivety decreased in the process (see 5.2), but in general calculating naivety with brute force does not appear to be feasible.

It would be greatly beneficial to find some sort of semi-invariant that behaves nicely with both multiplication and addition, or even addition alone. For example, let $f\colon R \to \mathbb{N}$ be a function such that:

1. $f(a+b) \leqslant f(a) + f(b)$
2. $f(ab) \leqslant f(a)f(b)$
3. for each $n \in \mathbb{N}$, the set $\{r : f(r) = a\}$ is finite.

If we had such a function f and a given $c \in AB$, we could determine the naivety of c by checking all representations such that $f(a_i) \leqslant f(c)$ and $f(b_i) \leqslant f(c)$. Due to property 3., we would only need to check finitely many representations, even if A and B are infinite. Of course we could define properties 1. and 2. somewhat differently, but even then finding such a function appears to be difficult, if not impossible for most rings.

None of the naturally-defined functions seem to be of much use. For example, the degree of a polynomial (over an integral domain) does not increase when multiplying by another polynomial—but it can decrease arbitrarily with addition (although hopefully some form of the reasoning from 5.3 could catch such cases). Similarly, the norm in algebraic integer rings ([1], p. 414) is multiplicative, which is a very nice property, but again—naivety is actually more of an additive phenomenon. Finding functions that behave nicely with addition seems generally much harder.

Calculating based naivety with brute force may actually be harder than calculating regular naivety—while the latter can keep adding $A \circ B$ to itself one iteration at a time (see next subsection), checking each of the $|B|^{\mathcal{N}^B(A,B)}$ possible bases requires substituting $|A|^{\mathcal{N}^B(A,B)}$ sets of coefficients every time (and multiplication, which is usually slower). However, this program may be lucky quite often, finding a valid basis very quickly, especially if we can provide it with good heuristics to let it start with the most promising potential bases.

Nonetheless, this does not mean that computers are of no use altogether. For example, the density in 5.1 was calculated using a simple Monte Carlo algorithm. Hopefully, as more estimates and theorems are discovered, more calculations will be possible to automate, or outright avoid.

4.2.2 Implementing a computer program

Writing a simple program to calculate naivety for finite ideals is not particularly difficult. Checking each representation would be too slow, but we can take advantage of "stratification" (see subsection 5.1)—$A \circ B$ is the set of all elements of naivety 1 (and zero), $(A \circ B) + (A \circ B)$ is the set of all elements of naivety 1 and 2 etc. That means that we can simply generate $A \circ B$, mark all of its elements as having naivety 1, then calculate $X_2 = (A \circ B) + (A \circ B)$ (by simply performing all pairwise additions), mark all its elements that are still unmarked as having naivety 2, calculate $X_3 = X_2 + (A \circ B)$ and so on. Note that we need to know AB beforehand (to prepare the array which will contain the naivety of each element). We also need to know when to terminate the process—in most cases, the generator bound provides a good stopping condition, but we can also check whether X_{i+1} is any bigger than X_i (since we need to perform all additions anyway) or check whether each element of AB already has a naivety assigned. The fact that this program calculates naivety of each element can be really useful for analyzing the additive structure—and I have not found a way to calculate the general naivety faster.

Using an object-oriented language is recommended, since we can easily input different ideals and rings into the same chassis. For calculating certain examples in this thesis, I implemented the above concept in Python—due to both the ease of overloading operators such as $+$ and $*$, and the general simplicity of its code. For most examples, the difference in speed as compared to a faster language would not change much—see for instance the huge polynomial growth in example 14, where even $p = 7$ would take several days. Even storing the results can prove problematic—human-readable text files can easily reach dozens of gigabytes.

5 Ideas and conjectures

This section contains the most promising leads that could result in significant advancements if studied more deeply. Some of them propose a non-directly-algebraic outlook, in an attempt to broaden the set of possible approaches to the problem. At this point, it is hard to judge which one is the most likely to be the right way forward, and it is quite likely that true advancement will require a combination of them, or even one that I have not yet considered. Nonetheless, they provide stems from which new ideas can blossom.

5.1 Stratification

By $X+Y$ we denote the sum set $\{x+y : x \in X, y \in Y\}$. By iterated sums of a set we mean X, $X+X$, $X+X+X$ and so on.

Despite using many terms related to multiplication, naivety is primarily an additive phenomenon—we take X, a subset of an additive (abelian) group, which acts as a sort of "seed" or "motherlode", and then build the iterations $X+X$, $X+X+X$ and so on, which are the "layers" or "strata". The knowledge that $X = A \circ B$ for some ideals, or even that multiplication exists, is not needed to define and study the problem. Of course, absorptivity is an extremely strong property which we would like to use—for instance it reflects the whole ring's structure inside each absorptive set—but it is not strictly necessary. Technically, commutativity or group properties (other that associativity) do not seem to be strictly necessary either.

Such a perspective has a few benefits: most notably, it is universal, potentially allowing us to answer problems unrelated to rings, as well as use more general methods of additive combinatorics (see [4]), some of which are mentioned below. It has two significant downsides, however: we lose the strong properties related to multiplication, and most methods of additive combinatorics use the notion of the size of various sets, as we shall now see. We will discuss this problem later.

Tao and Vu's book defines the *doubling constant* of a set: $\sigma[A] = \frac{|A+A|}{|A|}$, which is meant to measure the "additive disorder" of the set. A regular set, such as an arithmetic progression, will have a small doubling constant, while for a "generic" or "random" set it may reach $\frac{1}{2}(|A|+1)$ ([4], p. 57). For the purpose of measuring strata growth, we would likely want to calculate the similar number $\frac{|S+X|}{|S|}$, where $S = X + .. + X$ is one of the strata. Showing some sort of bound on this number—for example that it decreases as we take bigger strata—could help provide strong bounds on naivety.

Other definitions worth mentioning are that of *additive energy* and *Ruzsa distance*, both defined between two sets. The former is simply the number of non-unique addition results: $E(A,B) = |\{(a,a',b,b') \in A \times A \times B \times B : a+b = a'+b'\}|$, while the latter is defined as

$$d(A,B) = \log \frac{|A-B|}{|A|^{1/2}|B|^{1/2}}.$$

Pairs of sets with small distance or big additive energy have a lot of additive structure in common. We would likely want to study the distance or energy between the seed and the strata, although attempting to measure them between two particular stratums may yield some results as well. Studying the "distribution" of additive energy, i.e. which numbers in the sum set are achieved in how many different ways, could also reveal certain patterns (such as those related to the density described below).

Using these definitions, [4] provides a number of lemmas that give bounds on iterated sum sets (chapter 2). The iterated sum set bounds in chapter 2 are somewhat similar to the question of naivety, except in a "non-limited" setting, where the iterated sets generally keep growing. Passing from the non-limited to the limited setting may not be too hard—if we take some (finite) subset X of the additive group of integers and consider the iterated sums of it $(X, X+X, X+X+X, \dots)$, it is quite likely that after a while it will have a strongly structured mid-section (an arithmetic progression, typically just consecutive numbers), and only the extremes will be more disorganized. Ignoring this structured section may hopefully "limit" the problem sufficiently even if the additive group we are working in is infinite. For a formalization of this intuition see [4] (section 4.7 and chapter 12).

One idea which I have not encountered anywhere is trying to "cull" the strata. Given a stratum S, we would like to determine the smallest possible $S' \subset S$ such that $S+X = S'+X$. We can even go further: maybe there is some $S'' \subset S$ such that $S''+X \neq S+X$, but $S''+X+X = S+X+X$. We may even attempt to cull the seed itself. In this way, we could attempt to determine which elements are actually necessary, and which are just variants of others (of course it is quite likely that there will be a few different minimal sets with this property). This idea seems rather strongly correlated with absorptivity—it is quite likely that at least the integer multiples of other elements could be culled quite commonly, since they can be created using addition alone (although care must be taken to avoid increasing the required amount of summands).

As we have seen, methods of additive combinatorics generally rely on the notion of the size of sets—usually simply their cardinality. This is a serious problem, since most rings (and ideals therein) are infinite. Of the examples provided, only examples 6, 13 and 14 are finite. Of course sometimes we may force an example to be finite by using quotients, but it does not always preserve the additive structure (see 5.2). On $\mathbb{Z}$, we can define the natural density of a set by

$$\delta(A) = \lim_{n\to\infty} \frac{|\{a : a \in A, |a| \leqslant n\}|}{n}.$$

This can be generalized to other rings: for polynomials and other rings with structure similar to $\mathbb{Z}^n$, we may expand the above definition in one of the natural ways: iterating limits (one for each dimension), or bounding each coordinate by the same n. For instance, take the ring $\mathbb{Z}[x]$ and the ideals $A = (x, p), B = (x, q)$ (where p, q are distinct primes). I wrote a simple Monte Carlo program that chose a random polynomial of degree $\leqslant d$ by uniformly generating $d+1$ coefficients from the (integer) interval $[-M, M]$. Then, it checked whether that polynomial is in $A \circ B$ by finding its decomposition into irreducible polynomials and checking the divisibility of their constant terms by p and q. The resulting density was consistent with the formula

$$\delta(A \circ B) = \frac{1}{pq} \cdot \left(\left(\frac{1}{p}\right)^d + \left(\frac{1}{q}\right)^d - \left(\frac{1}{pq}\right)^d \right).$$

This formula gives exactly the density of "simple" polynomials from $A \circ B$—those that are products of either p or q by some element of the other ideal (by the inclusion-exclusion principle). Moreover, culling all other polynomials from $A \circ B$ does not increase the naivety—since we can set any coefficient we want for each degree separately, as p and q are coprime. This means that p and q are a sort of "naive basis taken from both ideals" (5.6 discusses a similar concept).

Of note is also the fact that when the limit M was small, the calculated density of $A \circ B$ was visibly higher, implying that "complex" polynomials are more common when the coefficients are close to 0. The density of the entire $AB = (x, pq)$ (limited to degree $\leqslant d$) is obviously equal to $\frac{1}{pq}$ regardless of d, and the density of $A \circ B$ is arbitrarily small for big values of d, so density can grow arbitrarily when taking the sum set—which, unluckily, makes it less useful. A similar behavior is observed for the set of prime numbers, which has density 0 with the above definition, but the set of sums of two primes has density 1 (which follows directly from [7]).

We could also try to extend the definition of density on $\mathbb{Z}$ into more general rings by "probing" sets with elements. If we take an element $r \in R$, then the set of its integer multiples $r, r + r, r + r + r, \ldots, -r, -r - r, \ldots$ can be identified with $\mathbb{Z}$ (or $\mathbb{Z}_p$, which makes density simply a finite ratio). To measure a set $A \subset R$, we may see how many of these multiples lie in A, and use the aforementioned definition of density on it. A likely conjecture is that—under reasonable assumptions—the set of resulting densities (for varying r and a fixed A) that are not 0 will have a well-defined positive infimum, which we may call the density of A (we cannot simply choose a single universal r to probe with, since for instance the set of even numbers has density $\frac{1}{2}$ if probed with 1, but density 1 if probed with 2—however probing all sets with a fixed r may yield some results). If we manage to find a good definition of density on another ring that commonly has an image in other rings, we could also use multiples by it instead of $\mathbb{Z}$. Absorptivity should be extremely helpful for such a definition of density, as it gives the set a regularity in terms of multiples of specific elements.

The aforementioned problem with this density growing unpredictably when taking the sum set means that it cannot be directly substituted for cardinality in additive combinatorics lemmas, but nonetheless it may turn out useful, especially if it is possible to calculate it using Monte Carlo methods in other rings as well.

If the perspective presented in this section ever evolves into an actual stream of research, I would like to propose the name "limited additive combinatorics", referencing the fact that most commonly (at least in the case of naivety), the strata eventually stop growing. In fact, assuming that they do could provide a vital handhold for studying such problems without the benefits of having an absorptive set in a ring.

5.2 Quotient rings

Note that this section mixes quotient and homomorphism notations—the former is better for the intended intuition, but the latter is usually symbolically cleaner.

We have the simple observation 5, which tells us that passing to a quotient ring does not increase naivety. However, a bit more can be said about such a situation. Let R be a ring and A, B ideals in it, as usual, and let Q be any ideal in R (the kernel of a homomorphism f). We will be moving from R to the quotient ring R/Q, which is equivalent to setting every element of Q equal to 0. Obviously $(A/Q)(B/Q) = AB/Q$.

The homomorphism f partitions AB into equivalence classes (fibers) by the simple relation $c \sim d \iff f(c) = f(d)$. We will denote these fibers by $f^{-1}(c')$ (where $c' \in AB/Q$). We know from observation 5 that the naivety of each element of $f^{-1}(c')$ (over A, B) cannot be smaller than the naivety of c' over $A/Q, B/Q$. Moreover, we have the following:

Observation 13. The set $f^{-1}(c')$ contains some element with naivety precisely equal to $\mathcal{N}_{A/Q,B/Q}(c')$.

The proof is simple: we can push a minimal representation of c' back through f (in any of the possible ways) to get a representation of the required element, of the desired length.

If $AB \subseteq Q$ (or even $A \subseteq Q$ or $B \subseteq Q$), the whole situation becomes trivial, as $AB/Q = (0)$ (or at least one of $A/Q, B/Q$ is (0)). This means that there are—roughly speaking—five interesting cases:

1. $Q \subsetneq AB$
2. $Q \subsetneq A$ (and 1. does not hold)
3. $A \cap Q \neq (0)$, $B \cap Q \neq (0)$ (and 2. does not hold)
4. $A \cap Q \neq (0)$, $B \cap Q = (0)$
5. $(A \cup B) \cap Q = (0)$

Of course for cases 2 and 4 we may as well switch the roles of A and B, which changes little in a commutative ring. We could further subdivide these cases by specifying the relation of AB and Q. For the first case—whose assumption is intuitively strongest—we have the following lemma:

Lemma 14. Let $Q \subsetneq AB$. Assume the naiveties of elements of Q (over A, B) are bounded from above by l. Let $c' \in (AB/Q)$ and $\mathcal{N}_{A/Q,B/Q}(c') = k$. Then for any $c \in f^{-1}(c')$, we have $\mathcal{N}_{AB}(c) \leqslant k + l$.

Let d be the element of smallest naivety over A, B in $f^{-1}(c')$—we know that d exists from observation 13. Let $d = a_1b_1 + \cdots + a_kb_k$ be its minimal representation. Since c and d are in the same fiber of f, we know that there is a $q \in Q$ such that $c = d + q = a_1b_1 + \cdots + a_kb_k + q$. But q has a representation of length at most l. That means that the above equality expands to a representation of c of length at most $k + l$. Finally, this means that $\mathcal{N}(A, B) \leqslant \mathcal{N}(A/Q, B/Q) + l$.

This lemma could be used to get the bound on naivety in examples 4 and 7 from, respectively, examples 5 and 6 (using observation 11 to get $l = 1$). Especially in case of example 7, it is a much more painless method to get that bound (with the trade-off of not bounding based naivety).

This lemma also gives us the (probably unsurprising) intuition that if Q is a subideal of AB with small naivety, then the additive structures of AB and AB/Q are relatively similar. In a way, this defines which Q we can regard as "small". If we could find another (compatible) definition of smallness of Q, we could in turn determine which elements of AB have small naiveties.

Cases 2, 3, 4, and 5 do not have their own lemmas yet. Intuitively, one would expect that case 5 would either evade description entirely, or that when moving to a quotient by a Q that is completely disjoint with both A and B, the additive structure would not change significantly. We may however note that in case 2, we could first move to the quotient by $Q' = Q \cap AB$, which is case 1, and then to the quotient by $Q'' = Q/Q'$, whose intersection with AB/Q' is null. It is unclear whether such a two-step consideration would weaken any resulting bounds, but it may make use of lemmas with stronger assumptions.

This whole deliberation could provide new results in two ways: firstly, the partitions into fibers by different Qs could provide insights into the additive structure of AB—especially if many of those partitions are "independent" (meaning, for instance, that the intersections $f^{-1}(c) \cap g^{-1}(c) \cap \dots$ are small), as then the naivety of each element of AB is controlled by several varied bounds. Secondly, it could allow for naivety to be controlled with a somewhat category-theoretic approach, where we would start with some uncomplicated, partially universal ring (such as polynomials over something) and use the naivety in it to control the naivety in its quotient rings. Polynomials in infinitely many variables over $\mathbb{Z}$ are, technically speaking, a universal ring, but constructing all rings directly as quotients of it appears too impractical.

Due to the dependence on representations of elements, it seems less likely that this method could provide any strong estimates on based naivety. Nonetheless, a similar perpective is briefly mentioned in 5.5.

5.3 Folding

Let $c = a_1b_1 + \dots + a_kb_k$ be a minimal representation of c. Note that if for some i, j we had $a_i = a_j$, we could collect ("fold") two products into a single one: $a_ib_i + a_jb_j = a_i(b_i + b_j)$ (since $b_i + b_j$ is obviously in B), thus shortening the representation. Obviously the same applies if $b_i = b_j$. We can take this reasoning further—it is sufficient that $a_i = d_1a$ and $a_j = d_2a$ for some $a \in A$, as then we have $a_ib_i + a_jb_j = a(d_ib_i + d_jb_j)$, using both closure under addition and absorptivity of B. This means that a minimal representation may not have two a_i, a_j (or b_i, b_j) with a common divisor in their respective ideal.

Unfortunately, irreducible elements are quite common in most rings (and an irreducible a_i will obviously not have common divisors with anything), and even if a_i, a_j do have a common divisor, it need not lie in A. As a result, most non-minimal representations cannot be shortened—nor even detected—in this way, and this observation can only catch some obviously bad ones. However, the idea itself could be expanded further. Perhaps there are such α_i, α_j such that $(a_i+\alpha_i)b_i+(a_j+\alpha_j)b_j = a_ib_i+a_jb_j$ and $(a_i+\alpha_i), (a_j+\alpha_j)$ do have a common divisor in A? Perhaps there is some other adjustment possible? Perhaps adding two new (opposite) terms to the representation can trigger a "chain reaction" of folding?

Determining whether it is possible to fold a given representation—either using the above ideas, or some other method—could lead to easier methods of finding lower bounds on naivety. For instance, if one could prove that (for some specific A, B) as long as a representation is longer that some k, we may fold two of its elements, then it would imply that $\mathcal{N}(A, B) \leqslant k$. Since this perspective could likely utilize otherwise unused properties of the ring or specific ideals, such techniques could end up quite valuable for finding both upper and lower bounds on naivety. The downside is that they would likely be quite hard to generalize efficiently, depending on the specific qualities of each particular example—however, we may yet find a beautiful and general theorem as well.

5.4 Preimage in matrices

Let $A = (a_1, \ldots, a_n)$ and $B = (b_1, \ldots, b_k)$ be finitely generated ideals in a commutative ring R. We will write $\mathbf{a}$ for the vector $(a_1, \ldots, a_n)^\top$, and $\mathbf{b}$ analogously (all vectors are vertical by default). Let $\mathcal{M}_{n\times k}(R)$ be the set of $n \times k$ matrices over R. We define the function $F_{\mathbf{a},\mathbf{b}} \colon \mathcal{M}_{n\times k}(R) \to R$ by

$$F_{\mathbf{a},\mathbf{b}}(M) = \mathbf{a}^\top M \mathbf{b}.$$

This function is obviously "linear" over R, so in particular it is a homomorphism of the additive groups of both rings.

Let $\mathcal{O}_{n,k} = \left\{\mathbf{v}\mathbf{w}^\top : \mathbf{v} \in R^n, \mathbf{w} \in R^k\right\}$ be the set of matrices of rank 1 (and the zero matrix), i.e. those matrices that are outer products of vectors. The elements of $A \circ B$ are products of elements of A and B, which in turn are linear combinations of the generators. This means that

$$A\circ B = \left\{ \left(\sum_i r_i a_i\right) \cdot \left(\sum_j s_j b_j\right) \mid r_i, s_j \in R \right\} = \left\{ \sum_{i,j} a_i r_i s_j b_j \right\} = \left\{\mathbf{a}^\top \mathbf{r}\mathbf{s}^\top \mathbf{b}\right\} = \left\{F_{\mathbf{a},\mathbf{b}}(\mathbf{r}\mathbf{s}^\top)\right\}$$

or in other words

$$F^{-1}_{\mathbf{a},\mathbf{b}}[A \circ B] \supseteq \mathcal{O}_{n,k}.$$

This may look unimpressive, but note that while $A\circ B$ is obviously dependent on A and B, $\mathcal{O}_{n,k}$ depends only on n and k. This means that we have found a "universal preimage" for ideals in R that have up to n or k generators, respectively (we can add fake generators equal to 0 if they have less).

$\mathcal{M}_{n\times k}(R)$ is not a ring, but it is a module over R, and observation 5 still applies. That means a lot of the reasoning in 5.2 still applies as well. In particular, the preimage of c through $F_{\mathbf{a},\mathbf{b}}$ contains matrices of rank at least $\mathcal{N}(A,B)$—including at least one with exactly that rank. Obviously, $F^{-1}_{\mathbf{a},\mathbf{b}}[AB] = \mathcal{M}_{n\times k}(R)$, since AB is generated by the products $a_i b_j$. The fact that the rank of a matrix is bounded by either of its dimensions is a direct translation of the generator bound. However, once we have added $\mathcal{O}_{n,k}$ to itself $\mathcal{N}(A,B)$ times (which can be less than n and k), the image will already be all of AB—in fact, the image will always be stratified as if we were simply using $A \circ B$ as the seed (see 5.1) instead of using $\mathcal{O}_{n,k}$ and moving through $F_{\mathbf{a},\mathbf{b}}$.

Since $F_{\mathbf{a},\mathbf{b}}$ is an R-module homomorphism, the structural similarity is even deeper. The image of a submodule $\mathfrak{C}$ of $\mathcal{M}_{n\times k}(R)$ is an ideal in R. If $\mathcal{O}_{n,k} \subseteq \mathfrak{C}$, then $A \circ B \subseteq F_{\mathbf{a},\mathbf{b}}(\mathfrak{C})$, and conversely if $\mathcal{O}_{n,k} \supseteq \mathfrak{C}$ then $A \circ B \supseteq F_{\mathbf{a},\mathbf{b}}(\mathfrak{C})$. Of course $F_{\mathbf{a},\mathbf{b}}(\mathfrak{C})$ may be (0) or (1), but in general the partial order of ideals in R is a "flattening" of the partial order of submodules of $\mathcal{M}_{n\times k}(R)$.

The problem with this method is that the matrices are not necessarily square (which can be solved with fake generators), and that they are over a ring instead of a field. Take for instance example 9—even though its proof uses matrices, they are matrices over $\mathbb{C}$, and not over $R = \mathbb{C}[x_1, \ldots, x_n]$. This makes the matrices more complicated and necessitates re-checking popular facts (we cannot even interpret the rank of a matrix as the dimension of a linear space spanned by its columns). We could interpret them as matrices over the fraction field of R, but then one has to be careful, as not all (but possibly some) matrices with entries from outside R will give valid elements of AB—or even of R.

Despite these difficulties, this technique allows for controlling whole classes of ideals at once, which may be extremely helpful for determining the "naive properties" of the given ring as a whole. Moreover, the strong structural similarity and the analogue of observation 13 can help determine properties of elements that (in relation to A and B) determine a given element's naivety. Perhaps some module other than $\mathcal{M}_{n\times k}(R)$ could retain this "universality" while being easier to work with, but it seems most likely that matrices are the best option. Additionally, based naivety works quite well with this perspective (although it does not make use of known terms such as rank directly).

5.5 Based naivety bounds

In examples 4 to 7 and 9 to 11, the following curious property holds:

$$\mathcal{N} \geqslant \frac{1}{2}\mathcal{N}^B. \tag{1}$$

Moreover, quite commonly in these examples we have

$$\mathcal{N} = \mathcal{N}^B. \tag{2}$$

Although examples 3 and 8 show that neither of these facts is universal, they appear to be prevalent enough to warrant a conjecture (especially since those examples are somewhat artificial). It seems (1) and (2) may hold when A and B are sufficiently similar. Moreover, it looks like in examples 9 and 11 naivety is smaller than based naivety due to a combination of two properties—$\mathbb{C}$ has square roots of each element, and the sum of two squares over $\mathbb{C}$ is a product of two linear factors (which is a direct result of the existence of a square root of -1). Example 10 does not have the latter, but does have the former (in the sense that at least positive elements have square roots) and indeed it has $\mathcal{N} = \mathcal{N}^B$. I have been unable to determine naivety over $\mathbb{Q}(i)$, which would be interesting, since this field has the latter property, but not the former (over $\mathbb{Q}$ naivety is the same as over $\mathbb{R}$, as it cannot go higher, even though the former has neither property). Moreover, I believe that if we stopped setting the third degree equal to zero, we would get $\mathcal{N} = \mathcal{N}^B$ even over $\mathbb{C}$.

A potential proof that (in certain cases) $\mathcal{N} = \mathcal{N}^B$ would likely need to identify specific features (such as the existence of square roots or the existence of nontrivial roots of -1) which cause naivety to be able to be less than based naivety—intuitively, that should happen commonly, but examples show otherwise. On the other hand, the bound $\mathcal{N} \geqslant \frac{1}{2}\mathcal{N}^B$ seems quite intuitive, as each side has the same amount of "free terms". A potential proof could use some concept similar to dimension (similarly to example 11). As a side note, even though I tried multiple variations of example 11 (with or without various mixed terms), I did not manage to break (1).

Examples 4 and 7 seem to suggest that elements of the basis are commonly simple combinations of generators of B—sums with coefficients 0 or 1, even. While I strongly doubt that those elements are always this simple, they do serve a rather similar role as the generators, and an uncomplicated relationship is entirely possible. Perhaps some proof of the above propositions can be achieved by "searching" the space of combinations (simple or not) of the generators, for instance showing that under certain conditions either two generators can be used in the basis or their sum can, and iterating such a lemma to get a complete basis.

Alternatively, one could try to find a proof by assuming that the basis is bigger than $\mathcal{N}(A, B)$ (or $2 \cdot \mathcal{N}(A, B)$) and showing that it allows such basis to be reduced via methods similar to those described in 5.3. We could also try to control the ideal B' generated by the basis and its relation to B. It could also be beneficial to study the effect of moving to a quotient ring R/Q on based naivety—obviously if some of the basis elements end up being equal to zero, the based naivety goes down, but perhaps more can be said if we know the exact relationship of Q and B'.

Examples in which naivety is sharply between $\mathcal{N}^B$ and $\left\lceil \frac{1}{2}\mathcal{N}^B \right\rceil$ are rather rare—example 14 was only found by a brute force calculation (although the aforementioned one with $\mathbb{Q}(i)$ may end up with naivety being between as well). Since both (1) and (2) are linear bounds, once we have determined the classes of rings in which those two inequalities hold, one could expect based naivety to be symmetric in them—or perhaps the assumption that $\mathcal{N}^B(A, B) = \mathcal{N}^B(B, A)$ is needed to prove the inequalities. In either case, since based naivety is commonly easier to calculate than regular naivety, even a bound with a factor of 2 could prove rather useful, so this perspective is worth studying.

5.6 Multiple arguments

One might ask—can we define naivety for more than two ideals? As it turns out, that is not only possible, but there are two competing definitions, loosely mirroring those of tensor rank and slice rank.

For simplicity, we will define these variants of multiargument naivety for specific elements (the naivety of the whole product is the supremum of the naiveties of its elements). We show them for three ideals A, B, C, and refer the reader back to section 2.2 if their extension into more arguments is unclear.

The "tensor naivety" $\mathcal{N}^t_{ABC}(d)$ of an element of ABC is defined as the length of the shortest representation of the form $d = a_1b_1c_1 + a_2b_2c_2 + \cdots + a_kb_kc_k$ (where of course $a_i \in A, b_i \in B, c_i \in C$).

The "slice naivety" $\mathcal{N}^s$ is defined as the length of the shortest representation that uses "slices", i.e. products of the form $a[bc]$, $b[ac]$, $c[ab]$, where the brackets mean any element of, respectively, BC, AC, AB (and not just an element of the naive product). Note that if we only had one possible form for the slices—say, the first one—then we would simply be calculating regular naivety over two ideals A and BC.

The product ABC is unsurprisingly equal to $(AB)C$, and it is also the set of finite sums of elements of the naive product $A \circ B \circ C = (A \circ B) \circ C = \{abc : a \in A, b \in B, c \in C\}$. This means that both $\mathcal{N}^t$ and $\mathcal{N}^s$ are well-defined (and finite) for every element of ABC, and that any element that is not in ABC cannot be represented using their respective representations.

One could try to define multiargument based naivety as well—for the tensor version, we would simply be choosing the basis from the last ideal and each coefficient would be a product of elements of all the other ideals. For the slice version, a proper definition seems harder to find—perhaps we could say the "sliced off" factors, regardless of their ideals of origin, are to be chosen as the basis beforehand (this was already mentioned in 5.1). Note that such a definition does not agree with the standard definition on two arguments—although it may not be greater than the standard based naivety—but still appears to fulfil many of the basic properties. It may be worth studying in more depth even without considering multiple arguments.

We can write some simple observations regarding both definitions of multiargument naivety:

Observation 15. $\mathcal{N}^t(A_1, \ldots, A_n) \geqslant \mathcal{N}^s(A_1, .., A_n)$.

This follows from the fact that any tensor representation is also a slice representation.

Observation 16. $\mathcal{N}^s(A_1, \ldots, A_n) \leqslant \mathcal{N}(A_i, A_1 \ldots A_{i-1}A_{i+1} \ldots A_n)$.

Any representation over A_i and $A_1 \ldots A_{i-1}A_{i+1} \ldots A_n$ is obviously also a slice representation.

Observation 17. $\mathcal{N}^t(A,B,C) \geqslant \mathcal{N}(A,B)$.

Obviously $ABC \subseteq AB$. Any element of the form $a_ib_ic_i$ is, due to absorptivity of B, also of the form $a_ib'_i$, so this inequality holds even for particular elements. Of course it can be expanded to an arbitrary number of arguments (replacing the $\mathcal{N}$ by $\mathcal{N}^t$), as long as the left side has more than the right side.

Note that we cannot write a similar inequality for slice naivety—slice representations over A, B, C and normal representations over A, B both use products that the other side cannot. Similarly, we cannot hope to write an inequality between $\mathcal{N}^s(A_1, A_2, \ldots, A_n)$ and $\mathcal{N}^s(A_1A_2, A_3, A_4, \ldots, A_n)$—slicing off an element of A_1A_2 is valid only for the right side, but slicing off an element of $A_1 \setminus A_2$ is valid only for the left side.

Observation 18. $\mathcal{N}^t(A,B,C) \geqslant \mathcal{N}(AB,C)$.

Any element of the form $a_ib_ic_i$ is also of the form $(a_ib_i)c_i$, so this inequality holds even for particular elements. Intuitively speaking, multiplying A and B beforehand means we can use some high-naivety elements of AB without paying that cost in length.

Observation 19. $\mathcal{N}^t(A,B,C) \leqslant \mathcal{N}(A,B) \cdot \mathcal{N}(AB,C)$.

To represent a $d \in ABC$, first we represent it over AB, C as $d = [ab]_1c_1 + \cdots + [ab]_kc_k$ (where $k = \mathcal{N}(AB,C)$) and then each of the $[ab]_i$ over A, B (with length at most $\mathcal{N}(A,B)$), which gives us the desired bound. This reasoning can be expanded to show that

$$\mathcal{N}^t(A_1, \ldots, A_n) \leqslant \mathcal{N}(A_1, A_2) \cdot \mathcal{N}(A_1A_2, A_3) \cdot \mathcal{N}(A_1A_2A_3, A_4) \cdot \ldots \cdot \mathcal{N}(A_1 \ldots A_{n-1}, A_n).$$

Note that this remains true even if we reorder the ideals, thus getting a different "slicing order". We can make a conjecture that the minimum over all permutations (or, in fact, parenthetisations) is the actual value of $\mathcal{N}^t(A_1, \ldots, A_n)$, but (for unexplained reasons) I feel that it will not hold in many cases.

Observations 18 and 19 show that tensor naivety can be approximated (if not outright calculated) from regular naivety by drawing a binary tree, where the leaves are ideals, and each node is the product of its two children (which expands observation 19 even further). Then the tensor naivety of the whole product is no greater than the product of (regular) naiveties on each node, but also no smaller than each of these naiveties. Moreover, the tensor naivety of each element of the whole product is not smaller than its (regular) naivety over the product in each node. As the ideal product is associative, we can draw the tree in multiple ways, potentially getting different bounds. This, along with observation 17, means that if we can calculate the naiveties of some sort of "base" ideals, we could get a solid idea of how naivety (either tensor or regular) looks in the whole ring. For example, in a Dedekind ring all ideals factor (uniquely) into prime ideals. If the naivety of each pair of prime ideals was 1, then we would know that the naivety of any pair of ideals in this ring is also 1.

This perspective is definitely messy, and if we only care about getting results on regular, two-argument naivety, it will likely not be extremely productive, but it offers us another connection to the structure of the entire ring instead of focusing on specific pairs (or tuples) of ideals. Moreover, it can uncover ties with tensor rank and slice rank, connecting naivety to other branches of research.

6 Closing remarks

At the conclusion of this thesis, it is likely appropriate to ask the question: what next? Despite being somewhat messy and hard to control, naivety is an interesting question, which may hopefully inspire advances in commutative algebra, additive combinatorics, or perhaps even extremal combinatorics or some areas of computing. I believe it is worth studying in more depth.

This thesis points to a few possible directions: first of all, as painful as it may be, more examples need to be calculated to inspire or evaluate conjectures. More algebraic lemmas, and perhaps even theorems could be found. Similar problems need to be explored and their methods adjusted. Any of the perspectives from section 5 could yield results, so they need to be researched in depth, and their specific issues faced. The research could also be expanded into non-commutative rings or other algebraic structures both more general and specific. There is also a whole list of miscellaneous ideas that I deemed too undeveloped or far-fetched to put into this thesis. Improved methods of automated calculations could save some of the effort. And ultimately, it is more than likely that new ideas will appear along the way.

References

[1] Artin, M. (1991) *Algebra*, Prentice-Hall, Upper Sadle River

[2] Bik, A. (2021) *Strength of Polynomials*, paper presented at Mathematical Colloquium Bern (https://personal-homepages.mis.mpg.de/arbik/pdf/bern21.pdf, accessed 14.06.2022)

[3] Croot, E., Lev, V.F., Pach, P.P. (2017) *Progression-free sets in Z_n^4 are exponentially small*, Annals of Mathematics, vol. 185 issue 1 (p. 331-337)

[4] Tao, T., Vu, V.H. (2006) *Additive Combinatorics*, Cambridge University Press, Cambridge [Cambridge studies in advanced mathematics vol. 105]

[5] Landsberg, J.M (2012) *Tensors: Geometry and Applications*, American Mathematical Society, Providence [Graduate Studies in Mathematics vol. 128]

[6] Hillar, C.J.; Lim, L. (2013) *Most tensor problems are NP-Hard*, Journal of the ACM, vol. 60 issue 6 (p. 1–39)

[7] Montgomery, H. L.; Vaughan, R. C. (1975) *The exceptional set in Goldbach's problem*, Acta Arithmetica, vol. 27 (p. 353–370)