Goldbach Rings

Michael Nelson

Abstract

Let $\Bbbk$ be a field. We introduce and study an interesting infinite-dimensional $\Bbbk$-algebra G which we call the Goldbach ring. As the name suggests, the Goldbach ring is closely related to Goldbach's conjecture. Properties that G satisfies as a ring (such as whether or not it is an integral domain) may give us clues about Goldbach's conjecture itself.

1 Introduction

Let $\Bbbk$ be a field. We introduce and study an interesting infinite-dimensional $\Bbbk$-algebra which we call the Goldbach ring, which, as the name suggests, is closely related to Goldbach's conjecture. The Goldbach ring G is defined to be the quotient $G = R/I$ where

$$R = \Bbbk[\{x_p, x_{p+q} \mid p, q \text{ odd primes}\}]$$
$$I = \langle \{x_p x_q - x_{p+q} \mid p, q \text{ odd primes}\} \rangle$$

The Goldbach ring has the structure of a bi-graded $\Bbbk$-algebra meaning it can be decomposed as

$$G = \bigoplus_{n,d \geq 0} G_{n,d},$$

where the component $G_{n,d}$ in bi-degree $(n, d) \in \mathbb{N}^2$ is a finite-dimensional $\Bbbk$-vector space whose dimension we are interested in counting. For instance, Goldbach's conjecture is equivalent to the statement that $\dim_{\Bbbk} G_{2k,2} = 1$ for all $k \geq 3$. However this is really just a restatment of Goldbach's conjecture; what's more interesting and new in our view is the following conjecture which seems to hold in small examples:

Conjecture 1. *We have*

$$\dim_{\Bbbk} G_{n,d} \leq 1$$

for all $n, d \in \mathbb{N}$.

A counter-example to Conjecture (1) would be the existence of odd primes $p_1, \ldots, p_d$ and $q_1, \ldots, q_d$ such that

$$p_1 + \cdots + p_d = n = q_1 + \cdots + q_d$$

but $x_{p_1} \cdots x_{p_d} \neq x_{q_1} \cdots x_{q_d}$ in G. However we do not believe such a counter-example exists since. Indeed, based on our initial calculations, it seems that there are usually many ways to go from $x_{p_1} \cdots x_{p_d}$ to $x_{q_1} \cdots x_{q_d}$ by applying elementary Goldbach relations of the form $x_p x_q = x_{p+q}$. For another example, in $G_{36,4}$ we have $x_3^2 x_{11} x_{19} = x_5^2 x_{13}^2$ since

$$\begin{aligned} x_3^2 x_{11} x_{19} &= x_3 x_{11} x_{22} \\ &= x_3 x_5 x_{11} x_{17} \\ &= x_5 x_{11} x_{20} \\ &= x_5 x_7 x_{11} x_{13} \\ &= x_5 x_{13} x_{18} \\ &= x_5^2 x_{13}^2. \end{aligned}$$

There are many other paths we can take from $x_3^2 x_{11} x_{19}$ to $x_5^2 x_{13}^2$, however it turns out that this is the shortest path. Ultimately a solution to Conjecture (1) will involve tools and techniques from analytic number theory. What we find interesting is that Conjecture (1) also seems to involve a lot of commutative algebra as well. For example, if Conjecture (1) is true, then it woud imply that G is an integral domain. Conversely, one can show that if G is an integral domain and Conjecture (1) holds for n, d sufficiently large, then Conjecture (1) is true.

A deeper relationship between Conjecture (1), anlaytic number theory, and commutative algebra is realized when one studies G as a limit

$$G = \varinjlim G^m$$

of bi-graded noetherian $\Bbbk$-algebras $G^m = R^m/I^m$, where

$$\begin{aligned} R^m &= \Bbbk[x_1, \ldots, x_m] \cap R \\ I^m &= \Bbbk[x_1, \ldots, x_m] \cap I. \end{aligned}$$

Indeed, for each m, we denote by $\delta(m)$ and $\rho(m)$ to be the R^m-depth and R^m-projective dimension of G^m respectively. Then the Auslander-Buchsbaum formula implies

$$\delta(2m) + \rho(2m) = \pi(2m) + m - \kappa(2m) - 3, \tag{1}$$

where $\pi(2m)$ is the usual prime-counting function which counts the number of primes $\leq 2m$ and where $\kappa(2m)$ counts then number of positive even numbers $\leq 2m$ that are coutner-examples to Goldbach's conjecture.

2 $\mathcal{A}$-Supported Goldbach Rings

Let $\mathcal{A}$ be a subset of the positive odd integers and set $\mathcal{C} := \mathcal{A} + \mathcal{A} = \{a + b \mid a, b \in \mathcal{A}\}$. We set

$$\begin{aligned} R_{\mathcal{A}} &= \Bbbk[\{x_a, x_c \mid a \in \mathcal{A}, c \in \mathcal{C}\}] \\ I_{\mathcal{A}} &= \langle \{x_a x_b - x_{a+b} \mid a, b \in \mathcal{A}\} \rangle \\ G_{\mathcal{A}} &= R_{\mathcal{A}}/I_{\mathcal{A}}. \end{aligned}$$

We will refer to $G_{\mathcal{A}}$ as the **$\mathcal{A}$-supported Goldbach ring**. We simplify our notation by writing $\{x_a, x_c\}$ to denote the set $\{x_a, x_c \mid a \in \mathcal{A}, c \in \mathcal{C}\}$. Similarly we write $\{x_a x_b - x_{a+b}\}$ to denote the set $\{x_a x_b - x_{a+b} \mid a, b \in \mathcal{A}\}$. We often simplify our notation even further by dropping $\mathcal{A}$ from our notation whenever it is clear from context. For instance, we write "G" instead of "$G_{\mathcal{A}}$" when it's understood that G is the $\mathcal{A}$-supported Goldbach ring. Similarly, if we write "let G be the $\mathcal{A}$-supported Golbach ring", then it's understood that $\mathcal{A}$ is a subset of the positive odd integers and that $\mathcal{C} = \mathcal{A} + \mathcal{A}$.

2.1 Representing Monomials

We will denote by $\mathcal{M} = \mathcal{M}_{\mathcal{A}}$ to be the set of all monomials in $R = R_{\mathcal{A}}$. There are two ways we can represent monomials in R. The first way is as a finite product of the indeterminates $\{x_a, x_c\}$, namely, a monomial can be expressed in the form

$$x_{\boldsymbol{a}} x_{\boldsymbol{c}} := x_{a_1} \cdots x_{a_r} x_{c_1} \cdots x_{c_s}$$

where $\boldsymbol{a} = a_1, \ldots, a_r$ is a sequence of elements in $\mathcal{A}$ (not necessarily distinct, but often we assume $a_1 \leq \cdots \leq a_r$) and $\boldsymbol{c} = c_1, \ldots, c_s$ is a sequence of elements in $\mathcal{C}$ (again not necessarily distinct, but often we assume $c_1 \leq \cdots \leq c_s$). We will use this way of representing monomials to give R a nice bi-graded structure. The second way of representing monomials is described as follows: given a function $\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0}$, we define its **support**, denoted $\operatorname{supp} \alpha$, to be the set

$$\operatorname{supp} \alpha = \{m \in \mathbb{N} \mid \alpha(m) \neq 0\}.$$

We denote by $\mathcal{F} = \mathcal{F}_{\mathcal{A}}$ to be the set

$$\mathcal{F} = \{\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0} \mid \operatorname{supp} \alpha \text{ is finite and contained in } \{x_a, x_c\}\}.$$

Thus if $\alpha \in \mathcal{F}$, then α takes value 0 zero almost everywhere, and the only places where it is nonzero is at an element in $\{x_a, x_c\}$. Then there is a bijection from $\mathcal{F}$ to $\mathcal{M}$ given by assigning $\alpha \in \mathcal{F}$ to the monomial

$$x^{\alpha} := \prod_{m \in \mathbb{N}} x_m^{\alpha(m)} = \prod_{m \in \operatorname{supp} \alpha} x_m^{\alpha(m)}.$$

For instance, suppose $\alpha \colon \mathbb{N} \to \mathbb{Z}_{\geq 0}$ is defined by

$$\alpha(m) = \begin{cases} 3 & \text{if } m = 2 \\ 2 & \text{if } m = 6 \\ 4 & \text{if } m = 11 \\ 0 & \text{if } m \in \mathbb{N} \backslash \{2, 6, 11\} \end{cases}$$

Then $x^\alpha = x_3^3 x_6^2 x_{11}^4$ and $\operatorname{supp} x^\alpha = \{2, 6, 11\}$. This second way of expressing monimals gives us a cleaner way of expressing nonzero polynomials in R, namely, every nonzero polynomial $f \in R$ can be expressed in the form

$$f = a_1 x^{\alpha_1} + \cdots + a_n x^{\alpha_n}$$

for unique $a_1, \ldots a_n \in \Bbbk$ and for unique $\alpha_1, \ldots, \alpha_n \in \mathcal{F}$. We often pass back and forth between functions $\alpha \in \mathcal{F}$ and monomials $x^\alpha \in \mathcal{M}$. For instance, given a monomial $x^\alpha \in \mathcal{M}$, we define its **support**, denoted $\operatorname{supp} x^\alpha$, to be $\operatorname{supp} x^\alpha = \operatorname{supp} \alpha$, and etc...

2.2 The Bi-Graded $\Bbbk$-Structure on R and G

We give R and G a bi-graded $\Bbbk$-structure as follows: we define $\deg_1 \colon \mathcal{M} \to \mathbb{N}$ and $\deg_2 \colon \mathcal{M} \to \mathbb{N}$ by

$$\deg_1(x_{\boldsymbol{a}} x_{\boldsymbol{c}}) = \sum_{i=1}^{r} a_i + \sum_{j=1}^{s} c_j \quad \text{and} \quad \deg_2(x_{\boldsymbol{a}} x_{\boldsymbol{c}}) = r + 2s.$$

In particular, we have $\deg_1(x_a) = a$, $\deg_1(x_c) = c$, $\deg_2(x_a) = 1$, and $\deg_2(x_c) = 2$. For each $n, d \in \mathbb{N}$, we set

$$R_{n,d} = \operatorname{span}_\Bbbk \{x^\alpha \in \mathcal{M} \mid \deg_1(x^\alpha) = n \text{ and } \deg_2(x^\alpha) = d\}.$$

Then we have a decomposition of R into $\Bbbk$-vector spaces:

$$R = \bigoplus_{n,d \in \mathbb{N}} R_{n,d},$$

which gives R a bi-graded $\Bbbk$-structure. Since I is homogeneous with respect to this bi-grading, G inherits a bi-graded $\Bbbk$-structure, induced by the one on R:

$$G = \bigoplus_{n,d \in \mathbb{N}} G_{n,d}.$$

We set $\Delta_{n,d} = \dim_\Bbbk R_{n,d}$ and $\delta_{n,d} = \dim_\Bbbk G_{n,d}$. Thus $\Delta_{n,d}$ counts the number of ways we can express n as a sum

$$n = a_1 + \cdots + a_r + c_1 + \cdots + c_s$$

where $a_1, \ldots, a_r \in \mathcal{A}$, $c_1, \ldots, c_s \in \mathcal{C}$, and $d = r + s$. Whenever we have $\Delta_{n,d} \geq 1$, then we say (n, d) is a **good pair**. In this case, we are very interested in determining whether or not $\delta_{n,d} = 1$ for $\delta_{n,d} > 1$. Intuitively, we have $\delta_{n,d} = 1$ when $\mathcal{A}$ is sufficiently "dense" in $\mathbb{N}$ and we have $\delta_{n,d} > 1$ whenever $\mathcal{A}$ is very "sparse" in $\mathbb{N}$.

2.3 Constructing the Minimal R-Free Resolution of G

We now build the minimal R-free resolution of G as follows: first, for each $m \geq 1$, we define the m**th approximation** of R, I, and G to be:

$$\begin{aligned} R^m &= \Bbbk[\{x_a, x_c \mid a, c \leq m\}] \\ I^m &= \langle \{x_a x_b - x_{a+b} \mid a + b \leq m\} \rangle \\ G^m &= R^m / I^m. \end{aligned}$$

Again, R^m and G^m have bi-graded $\Bbbk$-structures:

$$R^m = \bigoplus_{n,d} R^m_{n,d} \quad \text{and} \quad G^m = \bigoplus_{n,d} G^m_{n,d}.$$

Recall that if $x_a x_c \in R^m_n$, then we must have $a + c = n$ and $a, c \leq m$. In particular, if $m \geq n$ then we have $R^m_n = R^n_n = R_n$. Similarly, if $m \geq n$ then we have $G^m_n = G^n_n = G_n$. Thus we have directed systems

$$(R^m)_{m \geq 1} \quad \text{and} \quad (G^m)_{m \geq 1}$$

of bi-graded rings (with the obvious ring homomorphisms) where the bi-graded components $R^m_{n,d}$ and $G^m_{n,d}$ in bi-graded degree (n, d) stabilizes to $R_{n,d}$ and $G_{n,d}$ respectively whenever m is sufficiently large (for example $m \geq n$). It follows that

$$R = \varinjlim R^m \quad \text{and} \quad G = \varinjlim G^m$$

as bi-graded direct limits.

Next we let $F^m = F^m_{\mathcal{A}}$ be the minimal bi-graded R^m-free resolution of G^m (where F^m is necessarily finite since R^m and G^m are noetherian). We set

$$\varepsilon(m) = \varepsilon_{\mathcal{A}}(m) := \operatorname{depth}_{R^m} G^m \quad \text{and} \quad \rho(m) = \rho_{\mathcal{A}}(m) := \operatorname{pd}_{R^m} G^m = \operatorname{length} F^m.$$

Note that these quantities are intrinsic to R^m and G^m (and not R and G). By the Auslander-Buchsbaum formula we have

$$\rho(m) + \varepsilon(m) = \pi_{\mathcal{A}\cup\mathcal{C}}(m) := \#\{a, c \in \mathcal{A} \cup \mathcal{C} \mid a, c \leq m\}. \tag{2}$$

Note that F^m has the structure of a bi-graded $\Bbbk$-complex, meaning we have a decomposition of $\Bbbk$-complexes:

$$F^m = \bigoplus_{n,d} F^m_{n,d},$$

where $F^m_{n,d}$ is a finite $\Bbbk$-subcomplex of F^m which minimially resolves $G^m_{n,d}$, meaning the augmented complex

$$\widetilde{F}^m_{n,d} := \cdots \to F^m_{i,n,d} \to F^m_{i-1,n,d} \to \cdots \to F^m_{1,n,d} \to R^m_{n,d} \to G^m_{n,d} \to 0$$

is exact and where the ith bi-graded Betti number of G^m in bi-degree (n, d) is given by

$$\beta^m_{i,n,d} := \dim_{\Bbbk} \operatorname{Tor}_i^{R^m}(G^m, \Bbbk)_{n,d} = \dim_{\Bbbk}(F^m_{i,n,d}).$$

Furthermore, since $R^m_n = R^n_n$ and $G^m_n = G^n_n$ whenever $m \geq n$, we see that $F^m_n = F^n_n$ whenever $m \geq n$. Thus if we *define* $F_{\mathcal{A}} = F$ to be the direct limit of bi-graded $\Bbbk$-complexes

$$F := \varinjlim F^m,$$

then F is a bi-graded R-free resolution of G which has the following bi-graded $\Bbbk$-complex structure:

$$F = \bigoplus_{n,d} F_{n,d} = \bigoplus_{n,d} F^n_{n,d}.$$

In particular, if m is sufficiently large, then we see that $\beta^m_{i,n,d} = \beta_{i,n,d}$ where

$$\beta_{i,n,d} := \dim_{\Bbbk} \operatorname{Tor}_i^{R}(G, \Bbbk)_{n,d} = \dim_{\Bbbk}(F_{i,n,d})$$

is called the ith bi-graded Betti number of G in bi-degree (n, d). Thus, unlike the quantities $\varepsilon(m)$ and $\rho(m)$, the quantitiy $\beta^m_{i,n,d}$ is actually *intrinsic* to R and G (and not just R^m and G^m) when m is sufficiently large.

Theorem 2.1. *We have $\delta_{n,d} = \chi(F_{n,d})$. In other words, we have*

$$\delta_{n,d} = \Delta_{n,d} - \sum_{i=1}^{\infty} (-1)^i \beta_{i,n,d} = \sum_{i=0}^{\infty} (-1)^i \dim_{\Bbbk} \operatorname{Tor}_i^{R}(G, \Bbbk)_{n,d}, \tag{3}$$

where the sum on the right (3) is finite.

Finally, we want to build the minimal R-free resolution F of G using the minimal bi-graded R^m-free resolutions F^m of G^m. Here, F^m has the structure of a bi-graded $\Bbbk$-complex, meaning it decomposes as a direct sum

$$F^m = \bigoplus_{n,d} F^m_{n,d}$$

where the component $F^m_{n,d}$ is bi-degree (n, d) is a $\Bbbk$-complex. The ith bi-graded Betti number of G^m in bi-degree (n, d) is gien given by

$$\beta^m_{i,n,d} = \dim_{\Bbbk} \operatorname{Tor}_i^{R^m}(G^m, \Bbbk)_{n,d} = \dim_{\Bbbk}(F^m_{i,n,d}).$$

The canoical maps $G^m \to G^{m+1}$ induce comparison maps $F^m \to F^{m+1}$ which we may take to be inclusion maps which respect to the bi-graded structure. Furthermore, since $R^m_n = R^n_n$ and $G^m_n = G^n_n$ whenever $m \geq n$, we see that $F^m_n = F^n_n$ whenever $m \geq n$. Thus we can define F to be the direct limit of bi-graded $\Bbbk$-complexes

$$F := \varinjlim F^m,$$

then F is a bi-graded R-free resolution of G which has the following bi-graded $\Bbbk$-complex structure:

$$F = \bigoplus_{n,d} F_{n,d} = \bigoplus_{n,d} F^n_{n,d}.$$

In particular, if m is sufficiently large, then we see that $\beta_{i,n,d}^m = \beta_{i,n,d}$ where

$$\beta_{i,n,d} := \dim_{\Bbbk} \operatorname{Tor}_i^R(G, \Bbbk)_{n,d} = \dim_{\Bbbk}(F_{i,n,d})$$

is called the ith bi-graded Betti number of G in bi-degree (n, d). Thus, unlike the quantities $\varepsilon(m)$ and $\rho(m)$, the quantitiy $\beta_{i,n,d}^m$ is actually intrinsic to R and G (and not just R^m and G^m) when m is sufficiently large.

Theorem 2.2. *We have* $\dim_{\Bbbk} G_{n,d} = \chi(F_{n,d})$. *In other words, we have*

$$\delta_{n,d} = \Delta_{n,d} - \sum_{i=1}^{\infty}(-1)^i \beta_{i,n,d} = \sum_{i=0}^{\infty}(-1)^i \dim_{\Bbbk} \operatorname{Tor}_i^R(G, \Bbbk)_{n,d}, \tag{4}$$

where the sum on the right (3) is finite.

3 The Goldbach Ring

We now consider the case where $\mathcal{A} = \{\text{positive odd primes}\}$. In this case, we have

$$\begin{aligned} R &= \Bbbk[\{x_p, x_{2k} \mid p \text{ odd prime and } k \in \mathbb{Z}_{\geq 3}\}] \\ I &= \langle \{x_p x_q - x_{p+q} \mid p, q \text{ odd primes}\} \rangle \\ G &= R/I. \end{aligned}$$

For obvious reasons, we call G the **Goldbach ring.** The homogeneous components of the form $R_{18,d}$ looks like:

$$\begin{aligned} \vdots &= \vdots \\ R_{18,7} &= 0 \\ R_{18,6} &= \Bbbk x_3^6 + \Bbbk x_3^4 x_6 + \Bbbk x_3^2 x_6^2 + \Bbbk x_6^3 \\ R_{18,5} &= 0 \\ R_{18,4} &= \Bbbk x_3^2 x_5 x_7 + \Bbbk x_3 x_5^3 + \Bbbk x_3^2 x_{12} + \cdots + \Bbbk x_5 x_6 x_7 + \Bbbk x_6 x_{12} + \Bbbk x_8 x_{10} \\ R_{18,3} &= 0 \\ R_{18,2} &= \Bbbk x_5 x_{13} + \Bbbk x_7 x_{11} + \Bbbk x_{18} \\ R_{18,1} &= 0 \\ \vdots &= \vdots \end{aligned}$$

Similarly, the homogeneous components of the form $R_{17,d}$ looks like:

$$\begin{aligned} \vdots &= \vdots \\ R_{17,6} &= 0 \\ R_{17,5} &= \Bbbk x_3^4 x_5 + \Bbbk x_3^3 x_8 + \Bbbk x_3^2 x_5 x_6 + \Bbbk x_3 x_6 x_8 + \Bbbk x_5 x_6^2 \\ R_{17,4} &= 0 \\ R_{17,3} &= \Bbbk x_3^2 x_{11} + \Bbbk x_3 x_7^2 + \Bbbk x_5^2 x_7 + \Bbbk x_6 x_{11} + \Bbbk x_3 x_{14} + \Bbbk x_7 x_{10} + \Bbbk x_5 x_{12} \\ R_{17,2} &= 0 \\ R_{17,1} &= \Bbbk x_{17} \\ R_{17,0} &= 0 \\ \vdots &= \vdots \end{aligned}$$

Staring at the homogeneous components above, we see that $\Delta_{18,4} = 9$ and $\Delta_{17,3} = 7$. More generally, $\Delta_{n,d}$ counts the number of ways we can express n as a sum:

$$n = p_1 + \cdots + p_r + 2(k_1 + \cdots + k_s), \tag{5}$$

where $p_1, \ldots, , p_r$ are odd primes, $k_1, \ldots, k_s \geq 3$, and $d = r + 2s$. Here are some basic facts about $\Delta_{n,d}$:

1. Assume n is even.

$$\text{we have } \begin{cases} \Delta_{n,d} \geq 1 & \text{if } d \text{ is even and } 2 \leq d \leq \lfloor n/3 \rfloor \\ \Delta_{0,0} = 1 & \\ \Delta_{n,d} = 0 & \text{else} \end{cases}$$

   Indeed, if d is even and satisfies $2 \leq d \leq \lfloor n/3 \rfloor$, then we have $\Delta_{n,d} \geq 1$ since we have the decomposition $n = (n - 6d) + 6d$.

2. Assume n is odd.

$$\text{we have } \begin{cases} \Delta_{n,d} \geq 1 & \text{if } d \text{ is odd and } 3 \leq d \leq \lfloor n/3 \rfloor \\ \Delta_{n,1} = 1 & \text{if } n \text{ is an odd prime} \\ \Delta_{n,d} = 0 & \text{else} \end{cases}$$

Indeed, if d is odd and satisfies $3 \leq d \leq \lfloor n/3 \rfloor$, then we have $\Delta_{n,d} \geq 1$ since we have the decomposition $n = (n-3-6d) + 6d + 3$.

Next, the homogeneous components of the form $G_{17,d}$ and $G_{18,d}$ looks like:

$$\begin{array}{cc} \vdots = \vdots & \vdots = \vdots \\ G_{17,6} = 0 & G_{18,6} = \Bbbk\overline{x}_3^6 \\ G_{17,5} = \Bbbk\overline{x}_3^4\overline{x}_5 & G_{18,5} = 0 \\ G_{17,4} = 0 & G_{18,4} = \Bbbk\overline{x}_3^2\overline{x}_5\overline{x}_7 \\ G_{17,3} = \Bbbk\overline{x}_3^2\overline{x}_{11} & G_{18,3} = 0 \\ G_{17,2} = 0 & G_{18,2} = \Bbbk\overline{x}_5\overline{x}_{13} \\ G_{17,1} = \Bbbk\overline{x}_{17} & G_{18,1} = 0 \\ \vdots = \vdots & \vdots = \vdots \end{array}$$

From what we've seen above, it is *very* tempting to consider the following conjecture:

Conjecture 2. *If n is even, then*

$$\textit{we have } \begin{cases} \delta_{n,d} = 1 & \textit{if } d \textit{ is even and } 2 \leq d \leq \lfloor n/3 \rfloor \\ \delta_{0,0} = 1 & \\ \delta_{n,d} = 0 & \textit{else} \end{cases}$$

If n is odd, then

$$\textit{we have } \begin{cases} \delta_{n,d} = 1 & \textit{if } d \textit{ is odd and } 3 \leq d \leq \lfloor n/3 \rfloor \\ \delta_{n,d} = 1 & \textit{if } p \textit{ is an odd prime} \\ \delta_{n,d} = 0 & \textit{else} \end{cases}$$

To get an idea of why we think this conjecture is true, suppose (n,d) is a good pair and let x^α and x^β are two monomials in $R_{n,d}$. Then we'd like to show $\overline{x}^\alpha = \overline{x}^\beta$ in $G_{n,d}$. There are two issues to consider:

1. First of all, we'd like to represent each basis element in $G_{n,d}$ by a monomial of the form $x_{\boldsymbol{p}} = x_{p_1} \cdots x_{p_d}$ where $\boldsymbol{p} = p_1, \ldots, p_d$ are d odd primes such that $n = p_1 + \cdots + p_d$. However being able to do this is essentially equivalent to Goldbach's Conjecture being true. Having said that, even if Goldbach's Conjecture is false, we can still represent the basis elements in $G_{n,d}$ by "nice" monomials in the following sense: Assume that Goldbach's Conjecture is not true. Then we represent each basis element in $G_{n,d}$ by a monomial of the form

$$x_{\boldsymbol{p}} x_{2\boldsymbol{\kappa}} = x_{p_1} \cdots x_{p_r} x_{2\kappa_1} \cdots x_{2\kappa_s} \tag{6}$$

where $2\boldsymbol{\kappa} = 2\kappa_1 < \cdots < 2\kappa_s$ are the first s positive even integers that are counterexamples to Goldbach's Conjecture, and where s is chosen to be minimal. Thus if x^α and x^β are two monomials in $R_{n,d}$ such $\overline{x}^\alpha = \overline{x}_{\boldsymbol{p}}\overline{x}_{2\boldsymbol{\kappa}}$ and $\overline{x}^\beta = \overline{x}_{\boldsymbol{q}}\overline{x}_{2\boldsymbol{\kappa}}$, then showing $\overline{x}^\alpha = \overline{x}^\beta$ is equivalent to showing $\overline{x}_{\boldsymbol{p}} = \overline{x}_{\boldsymbol{q}}$, so we are reduced to the case where we may assume that each basis element in $G_{n,d}$ can be represented by a monomial of the form $x_{\boldsymbol{p}}$.

2. Thus by the first point, we may assume that $\overline{x}^\alpha = \overline{x}_{\boldsymbol{p}}$ and $\overline{x}^\beta = \overline{x}_{\boldsymbol{q}}$ where $\boldsymbol{p} = p_1, \ldots, p_d$ and $\boldsymbol{q} = q_1, \ldots, q_d$ are d odd primes such that

$$p_1 + \cdots + p_d = n = q_1 + \cdots + q_d.$$

Even in this reduced case however, it is not clear why $\overline{x}_{\boldsymbol{p}} = \overline{x}_{\boldsymbol{q}}$. Indeed, in $G_{27,3}$, we have $\overline{x}_3\overline{x}_{11}\overline{x}_{13} = \overline{x}_5^2\overline{x}_{17}$, however it takes some work to show this:

$$\begin{aligned} \overline{x}_3\overline{x}_{11}\overline{x}_{13} &= \overline{x}_{11}\overline{x}_{16} \\ &= \overline{x}_5\overline{x}_{11}\overline{x}_{11} \\ &= \overline{x}_5\overline{x}_{22} \\ &= \overline{x}_5^2\overline{x}_{17}. \end{aligned}$$

Note that at each step in the computation above, we are only allowed to use a relation of the form $\overline{x}_p\overline{x}_q = \overline{x}_{p+q}$. For another example, in $G_{36,4}$ we have $\overline{x}_3^2\overline{x}_{11}\overline{x}_{19} = \overline{x}_5^2\overline{x}_{13}^2$ since

$$\begin{aligned}\overline{x}_3^2\overline{x}_{11}\overline{x}_{19} &= \overline{x}_3\overline{x}_{11}\overline{x}_{22}\\ &= \overline{x}_3\overline{x}_5\overline{x}_{11}\overline{x}_{17}\\ &= \overline{x}_5\overline{x}_{11}\overline{x}_{20}\\ &= \overline{x}_5\overline{x}_7\overline{x}_{11}\overline{x}_{13}\\ &= \overline{x}_5\overline{x}_{13}\overline{x}_{18}\\ &= \overline{x}_5^2\overline{x}_{13}^2.\end{aligned}$$

The path we took to get from $\overline{x}_3^2\overline{x}_{11}\overline{x}_{19}$ to $\overline{x}_5^2\overline{x}_{13}^2$ was longer than the path we took to get from $\overline{x}_3\overline{x}_{11}\overline{x}_{13}$ to $\overline{x}_5^2\overline{x}_{17}$, so one can imagine that for n and d large, the path from $x_{\boldsymbol{p}}$ to $x_{\boldsymbol{q}}$ may be even longer, however at the same time, there are *more* ways to get from $\overline{x}_3^2\overline{x}_{11}\overline{x}_{19}$ to $\overline{x}_5^2\overline{x}_{13}^2$ than there are to get from $\overline{x}_3\overline{x}_{11}\overline{x}_{13}$ to $\overline{x}_5^2\overline{x}_{17}$, and hence for n and d large, there should be more ways to get from $x_{\boldsymbol{p}}$ to $x_{\boldsymbol{q}}$ (as there are many such relations of the form $\overline{x}_p\overline{x}_q = \overline{x}_{p+q}$). In order to prove Conjecture (2), we only need to find *one* path from $x_{\boldsymbol{p}}$ to $x_{\boldsymbol{q}}$.

If Conjecture (2) is true, then G has a nice property as a ring:

Proposition 3.1. *Assume Conjecture (2) is true. Then G is an integral domain.*

Proof. Let $f, g \in G_{n,d} = \Bbbk\overline{x}^{\alpha}$ such that $fg = 0$ and express f and g as

$$f = a\overline{x}^{\alpha} \quad \text{and} \quad g = b\overline{x}^{\alpha}.$$

Then clearly since $\overline{x}^{2\alpha} \neq 0$, we must have $ab = 0$, which implies either $a = 0$ or $b = 0$ which implies either $f = 0$ or $g = 0$. □

Remark 1. Note that for m sufficiently large, G^m has lots and lots of zero-divisors. For instance, in G^{16}, we have $x_3x_5x_{13} = x_5^2x_{11} = x_3x_7x_{11}$ which implies

$$x_3(x_5x_{13} - x_7x_{11}) = 0.$$

Since $x_5x_{13} - x_7x_{11} \neq 0$ in G^{16}, we see that x_3 and $x_5x_{13} - x_7x_{11}$ form a zero-divisor pair. The ring homomorphism $G^{16} \to G^{18}$ kills this zero-divisor pair by sending $x_5x_{13} - x_7x_{11}$ to 0, however we pick up another zero-divisor pair in G^{20}: namely x_3 and $x_{11}x_{11} - x_5x_{17}$. Indeed, in G^{20} we have

$$\begin{aligned}x_3x_{11}x_{11} &= x_7x_7x_{11}\\ &= x_5x_7x_{13}\\ &= x_3x_5x_{17},\end{aligned}$$

but $x_{11}x_{11} - x_5x_{17} \neq 0$ in G^{20}. Again, the ring homomorphism $G^{20} \to G^{22}$ kills this zero-divisor pair since $x_{11}x_{11} - x_5x_{17}$ in G^{22}, however we may pick up more zero-divisors in G^{22}.

3.1 Expressing the Prime Counting Function in terms of Projective Dimension

Let us recall some notation we developed in the case and explain what they look like here. For each $m \geq 1$, we have

$$\begin{aligned}R^m &= \Bbbk[\{x_p, x_{2k} \mid p, 2k \leq m\}]\\ I^m &= \langle\{x_px_q - x_{p+q} \mid p, q \leq m\}\rangle\\ G^m &= R^m/I^m\\ F^m &\text{ is the minimal } R^m\text{-free resolution of } G^m\\ F &\text{ is the minimal } R\text{-free resolution of } G\\ \varepsilon(m) &= \operatorname{depth}_{R^m}(G^m)\\ \rho(m) &= \operatorname{pd}_{R^m}(G^m) = \operatorname{length}(F^m)\end{aligned}$$

Note that (2) has a very nice interpretation in this case. Indeed, we have

$$\rho(2m) + \varepsilon(2m) = \pi(2m) + m - 3, \tag{7}$$

where π is the usual prime-counting function. For m sufficiently large, we should have

$$\varepsilon(2m) = \#\{p \mid m \leq p \leq 2m\}.$$

Indeed, the idea is that if $p_1, \ldots, p_d$ are all of the primes between m and $2m$, then it is easy to check that $\boldsymbol{x} = x_{p_1}, \ldots, x_{p_d}$ is a G^{2m}-regular sequence (the hard part is showing that this is in fact a maximal G^{2m}-regular sequence, however we will assume this is true for the moment). Thus we have $\pi(m) = \pi(2m) - \varepsilon(2m)$, and so we should be able to re-express (7) as

$$\pi(m) = \rho(2m) - m + 3. \tag{8}$$

For example, a calculation using a computer algebra program such as Singular shows $\rho(18) = 10$. Then since $\pi(9) = 4$, we have $4 = 10 - 9 + 3$, and thus (8) holds on the nose in this case.

3.1.1 Explicit Calculations of the $\mathbb{k}$-Complex $F_{n,d}$

Example 3.1. Let's describe $\widetilde{F}_{18,2}$ as a $\mathbb{k}$-complex. First, as a graded $\mathbb{k}$-vector space, we have

$$\begin{aligned}
\widetilde{F}_{1,18,2} &= \mathbb{k}e_{5,13} + \mathbb{k}e_{7,11} \\
\widetilde{F}_{0,18,2} &= R_{18,2} = \mathbb{k}x_5x_{13} + \mathbb{k}x_7x_{11} + \mathbb{k}x_{18} \\
\widetilde{F}_{-1,18,2} &= G_{18,2} = \mathbb{k}\overline{x}_5\overline{x}_{13},
\end{aligned}$$

and $\widetilde{F}_{i,18,2} = 0$ for all $i \neq -1, 0, 1$. The differential is the unique R-linear map defined by $\mathrm{d}(e_{5,13}) = x_5x_{13} - x_{18}$ and $\mathrm{d}(e_{7,11}) = x_7x_{13} - x_{18}$. After choosing ordered bases, we can express $\widetilde{F}_{18,2}$ in the form

$$0 \longrightarrow \mathbb{k}^2 \xrightarrow{\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ -1 & -1 \end{pmatrix}} \mathbb{k}^3 \xrightarrow{\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}} G_{18,2} \longrightarrow 0$$

As expected, we have

$$\delta_{18,2} = \chi(F_{18,2}) = 3 - 2 = 1.$$

.

Next, let's describe $\widetilde{F}_{23,3}$ as a $\mathbb{k}$-complex. First, as a graded $\mathbb{k}$-vector space, we have

$$\begin{aligned}
\widetilde{F}_{2,23,3} &= \mathbb{k}e_{5,7,11} \\
\widetilde{F}_{1,23,3} &= \mathbb{k}x_{13}e_{3,7} + \mathbb{k}x_{13}e_{5,5} + \mathbb{k}x_7e_{3,13} + \mathbb{k}x_7e_{5,11} + \mathbb{k}x_5e_{7,11} + \mathbb{k}x_5e_{5,13} \\
\widetilde{F}_{0,23,3} &= R_{23,3} = \mathbb{k}x_{13}x_{10} + \mathbb{k}x_7x_{16} + \mathbb{k}x_5x_{18} + \mathbb{k}x_5x_7x_{11} + \mathbb{k}x_3x_7x_{13} + \mathbb{k}x_5^2x_{13} \\
\widetilde{F}_{-1,23,3} &= G_{23,2} = \mathbb{k}\overline{x}_5\overline{x}_7\overline{x}_{11}
\end{aligned}$$

and $\widetilde{F}_{i,23,3} = 0$ for all $i \neq -1, 0, 1, 2$. The differential is the unique R-linear map defined by

$$\begin{aligned}
\mathrm{d}(e_{5,7,11}) &= x_5e_{7,11} - x_5e_{5,13} + x_{13}e_{5,5} - x_{13}e_{3,7} + x_7e_{3,13} - x_7e_{5,11} \\
\mathrm{d}(e_{3,7}) &= x_3x_7 - x_{10} \\
\mathrm{d}(e_{5,5}) &= x_5x_5 - x_{10} \\
\mathrm{d}(e_{3,13}) &= x_3x_{13} - x_{16} \\
\mathrm{d}(e_{5,11}) &= x_5x_{11} - x_{16} \\
\mathrm{d}(e_{7,11}) &= x_7x_{11} - x_{18} \\
\mathrm{d}(e_{5,13}) &= x_5x_{13} - x_{18}.
\end{aligned}$$

After choosing ordered basis, we can express $\widetilde{F}_{23,3}$ in the form

$$0 \longrightarrow \mathbb{k} \xrightarrow{\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}} \mathbb{k}^6 \xrightarrow{M} \mathbb{k}^6 \xrightarrow{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}} G_{23,3} \longrightarrow 0$$

where M is a matrix whose entries are either -1, 0, or 1.

3.2 Re-interpreting the Conjecture

From Theorem (2.2), we can express Conjecture (2) in another form:

Conjecture 3. *Assume (n,d) is a good pair. Then*

$$\sum_{i=0}^{\infty}(-1)^i \dim_{\Bbbk} \operatorname{Tor}_i^R(G,\Bbbk)_{n,d} = 1.$$

3.2.1 Monomial order

The following monomial order on $\mathcal{M}$ will be very useful for what follows. Let $x^\alpha = x_p x_{2k}$ and $x^{\alpha'} = x_{p'} x_{2k'}$ be two distinct monomials in $\mathcal{M}$. We say $x^\alpha \leq x^{\alpha'}$ if either

1. $\deg_1(x^\alpha) < \deg_1(x^{\alpha'})$ or;
2. $\deg_1(x^\alpha) = \deg_1(x^{\alpha'})$ and $\deg_2(x^\alpha) < \deg_2(x^{\alpha'})$ or;
3. $\deg_1(x^\alpha) = \deg_1(x^{\alpha'})$, $\deg_2(x^\alpha) < \deg_2(x^{\alpha'})$, and $x_{2k} <_{\text{lex}} x_{2k'}$ or;
4. $\deg_1(x^\alpha) = \deg_1(x^{\alpha'})$, $\deg_2(x^\alpha) < \deg_2(x^{\alpha'})$, $x_{2k} <_{\text{lex}} x_{2k'}$, and $x_p >_{\text{lex}} x_{p'}$.

Note that the first two conditions simply say that if $x^\alpha \in R_{n,d}$ and $x^{\alpha'} \in R_{n',d'}$, then $x^\alpha \leq x^{\alpha'}$ if either $n < n'$, or $n = n'$ and $d < d'$. In other words, the monomial order respects the bi-graded structure on R (every monomial in $R_{17,3}$ is strictly less than every monomial in $R_{17,5}$, and every monomial in $R_{17,5}$ is strictly less than every monomial in $R_{18,4}$). When the two monomials $x^\alpha = x_p x_{2k}$ and $x^{\alpha'} = x_{p'} x_{2k'}$ belong to the same homogeneous component $R_{n,d}$, then we use a lexicographical ordering where the even parts x_{2k} and $x_{2k'}$ take precedence over the prime parts x_p and $x_{p'}$. Thus in $R_{17,3}$, we have

$$x_3^2 x_{11} \leq x_3 x_7^2 \leq x_5^2 x_7 \leq x_{11} x_6 \leq x_7 x_{10} \leq x_5 x_{12} \leq x_3 x_{14}.$$

The idea here is that the monomials $x_3^2 x_{11}$, $x_3 x_7^2$, and $x_5^2 x_7$ have no even terms in them, so these should be the "lowest" terms

Extra Material

Let A be a finite abelian group (with the group operation denoted using multiplicative notation). We define

$$\begin{aligned} R_A &= \mathbb{Z}[\{X_a \mid a \in A\}] \\ I_A &= \langle \{X_a X_b - X_{ab} \mid a,b \in A\} \rangle \\ G_A &= R_A / I_A \end{aligned}$$

When A is understood from context, then we simplify notation by writing $R = R_A$, $I = I_A$, and $G = G_A$. We denote by x_a to be the coset in G with X_a as one of its representatives. Recall that the group ring $\mathbb{Z}[A]$ is a ring whose underlying set consists of all elements of the form $\sum_{a\in A} n_a[a]$ where $n_a \in \mathbb{Z}$. Note that we have an isomorphism $\mathbb{Z}[A] \simeq G$ induced by the map $[a] \mapsto x_a$. Now we homgenize everything

$$\begin{aligned} \widetilde{R} &= \mathbb{Z}[\{X_a, Z, \mid a \in A\}] \\ \widetilde{I} &= \langle \{X_a X_b - Z X_{ab} \mid a,b \in A\} \rangle \\ \widetilde{G} &= \widetilde{R} / \widetilde{I} \end{aligned}$$

Proposition 3.2. *The ideal $\widetilde{I}$ is minimally generated by a graded $\widetilde{R}$-sequence of length $|A|$.*

Proof. By the structure theorem of finite abelian groups we have an isomorphism of finite abelian groups

$$A \cong C_{q_1} \times \cdots \times C_{q_i} \times \cdots \times C_{q_k},$$

where the q_i are powers of (not necessarily distinct) prime numbers which are uniquely determined by A, and where C_{q_i} denotes the cyclic group of order q_i for all $1 \leq i \leq k$. In particular, there exists $a_1, \ldots, a_k \in A$ such that $\operatorname{ord} a_i = q_i$ for all i and such that every element in A has the form

$$a^{\boldsymbol{e}} := a_1^{e_1} \cdots a_i^{e_i} \cdots a_k^{e_k},$$

for unique $\boldsymbol{e} = (e_1, \ldots, e_k) \in \mathbb{N}^k$ where $0 \leq e_i < q_i$ for all $1 \leq i \leq k$ (whenever we write $a^{\boldsymbol{e}}$, it will always be understood that $0 \leq e_i < q_i$ for all $1 \leq i \leq k$) where $a^{(0,\ldots,0)} = 1$ in this notation. We claim that I_A is generated by the following polynomials:

$$\begin{aligned}
f_1 &= X_1 - X_{a_1}^{q_1} \\
f_{a_i} &= X_{a_i} - X_{a_i} X_{a_{i+1}}^{q_{i+1}} && 1 \leq i < k \\
f_{a_k} &= X_{a_k} - X_{a_k} X_1 \\
f_{a_i^{e_i} a_{i+1}^{e_{i+1}} \cdots a_k^{e_k}} &= X_{a_i^{e_i} a_{i+1}^{e_{i+1}} \cdots a_k^{e_k}} - X_{a_i}^{e_i} X_{a_{i+1}^{e_{i+1}}} \cdots X_{a_k^{e_k}} && 1 \leq i < j \leq k, \quad 2 \leq e_i < q_i, \quad 0 \leq e_j < q_j \\
f_{a_k^{e_k}} &= X_{a_k^{e_k}} - X_{a_k}^{e_k} && 2 \leq e_k \leq q_k
\end{aligned}$$

The graded version looks like

$$\begin{aligned}
f_1 &= Z^{q_1 - 1} X_1 - X_{a_1}^{q_1} \\
f_{a_i} &= X_{a_i} (Z^{q_{i+1}} - X_{a_{i+1}}^{q_{i+1}}) && 1 \leq i < k \\
f_{a_k} &= X_{a_k} (Z - X_1) \\
f_{a_i^{e_i} a_{i+1}^{e_{i+1}} \cdots a_k^{e_k}} &= Z^{e_i} X_{a_i^{e_i} a_{i+1}^{e_{i+1}} \cdots a_k^{e_k}} - X_{a_i}^{e_i} X_{a_{i+1}^{e_{i+1}}} \cdots X_{a_k^{e_k}} && 1 \leq i < j \leq k, \quad 2 \leq e_i < q_i, \quad 0 \leq e_j < q_j \\
f_{a_k^{e_k}} &= Z^{e_k - 1} X_{a_k^{e_k}} - X_{a_k}^{e_k} && 2 \leq e_k \leq q_k
\end{aligned}$$

Clearly we have a bijection $A \cong \{f_{a^{\boldsymbol{e}}} \mid a^{\boldsymbol{e}} \in A\}$. Fix $<$ to be the standard negative degree lexicographical ordering on the set of monomials of R where $X_{a^{\boldsymbol{e}}} > X_{a^{\boldsymbol{e}'}}$ if and only if $a^{\boldsymbol{e}} > a^{\boldsymbol{e}'}$. Thus we have

$$1 > X_1 > X_{a_1} > X_{a_2} > \cdots > X_{a_k} > X_1^2 > X_1 X_{a_1} > \cdots > X_1^3 > \ldots.$$

In particular, we see that $\mathrm{LT}(f_{a^{\boldsymbol{e}}}) = X_{a^{\boldsymbol{e}}}$. Note that if we localize $\langle \{f_{a^{\boldsymbol{e}}} \mid a^{\boldsymbol{e}} \in A\} \rangle$ at the maximal ideal $\mathfrak{m} = \langle \{\boldsymbol{X}_{a^{\boldsymbol{e}}}\} \rangle$, then we obtain $\langle \{f_{a^{\boldsymbol{e}}} \mid a^{\boldsymbol{e}} \in A\} \rangle = \mathfrak{m}$.

□