COMPUTATION OF GROSS-KEATING INVARIANTS

CHUL-HEE LEE

Abstract. The Gross-Keating invariant of a half-integral matrix over a $p$-adic integer ring is a fundamental concept in the study of quadratic forms, and has important applications for Siegel modular forms and arithmetic geometry. We introduce the Mathematica package computeGK, a computer program for calculating the Gross-Keating invariant and the Siegel series of a half-integral matrix over $\mathbb{Z}_p$, as well as other related quantities. As a by-product, we obtain a table of the arithmetic intersection numbers related to the classical modular polynomials using the explicit formula of Gross and Keating.

Introduction

In [GK93] Gross and Keating introduced an invariant of a ternary quadratic form over $\mathbb{Z}_p$ to express certain arithmetic intersection numbers of three modular correspondences explicitly. They also pointed out the observations of Kudla and Zagier that these numbers seem to be closely related to the central derivatives of the Fourier coefficients of the Siegel-Eisenstein series of weight 2 and degree 3, which gave rise to Kudla’s program [Kud97] connecting these objects in a more general setting.

Meanwhile, Katsurada obtained a recursive formula for the local Siegel series of the half-integral matrix $B$ of any degree over $\mathbb{Z}_p$ in [Kat99]. Katsurada’s formula is of central importance in the algorithmic calculation of the Fourier coefficients of the Siegel-Eisenstein series, and therefore has made a significant impact in the computational area of Siegel modular forms and the classification of even unimodular lattices in high dimensions [Kin03, KPSY18].

In [Wed07] Wedhorn expressed Katsurada’s formula for a half-integral matrix over $\mathbb{Z}_p$ of degree 3 using its Gross-Keating invariant. Recently, Ikeda and Katsurada [IK16] showed that the formula, for the half-integral matrix $B$ of any degree over any non-Archimedean local field of characteristic 0, can be reformulated in terms of an extended version of the Gross-Keating invariant of $B$, based on their foundational work [IK15]. It also implies that the extended Gross-Keating invariant, depending only on the equivalence class of $B$, completely determines the Siegel series of $B$. Thus, we can see that the
Gross-Keating invariant is quite fundamental from both theoretical and computational perspective.

In [CIKY17], Cho, Ikeda, Katsurada and Yamauchi obtained a family of formulas for computing the Gross-Keating invariants and related quantities for half-integral matrices over any finite extension of \( \mathbb{Z}_p \) for odd \( p \) and over any unramified finite extension of \( \mathbb{Z}_2 \). This has made an algorithmic treatment of the Gross-Keating invariant feasible for matrices of any degree.

In this work, we present the Mathematica package \texttt{computeGK}\footnote{The code is available at \url{https://github.com/chlee-0/computeGK}}, which implements these formulas for half-integral matrices over \( \mathbb{Z}_p \). With this program, we can compute the Gross-Keating invariant, a naive extended Gross-Keating datum, and the Siegel series of such a matrix. It also implements the explicit formula of Gross and Keating for the arithmetic intersection numbers, and we generate a table of them using the program. To the best of our knowledge, this is the first computer implementation to calculate the Gross-Keating invariants. There is a LISP code for the Siegel series, used in [Kin03, KPSY18] based on Katsurada’s formula [Kat99], but it is more specialized in computing the Fourier series of the Siegel-Eisenstein series, and does not address the Gross-Keating invariants; see Subsection 1.5 for more comments.

This paper is organized as follows. In Section 1 we recall the definition of the Gross-Keating invariant and the Siegel series for a half-integral matrix and review the key results for computing them. We also explain how to handle them in \texttt{computeGK} with examples. In Section 2 we explain some matrix reduction procedures and algorithms used within our program. In Section 3 we consider the formula of Gross and Keating for the arithmetic intersection number of three modular correspondences. We explain the details of how to use it for explicit calculations, and present some related tables generated by \texttt{computeGK}.

1. Gross-Keating invariants and Siegel series

In this section, we closely follow the presentation of [CIKY17] with minor modifications. We accompany our explanation with exemplary \texttt{computeGK} instructions.

1.1. Notation. Let \( p \in \mathbb{Z}_{\geq 0} \) be a prime, \( F = \mathbb{Q}_p \), and \( \mathfrak{o} = \mathbb{Z}_p \) its ring of integers. For \( a \in F^\times \), we write \( \text{ord}(a) = n \) if \( a \in p^n \mathfrak{o}^\times \), and call it the valuation of \( a \), and set \( \text{ord}(0) = \infty \). For two square matrices \( X \) and \( Y \) with entries in \( F \), we denote the matrix \( \begin{pmatrix} X & O \\ O & Y \end{pmatrix} \) by \( X \perp Y \). We denote the diagonal matrix \((b_1) \perp \ldots \perp (b_n)\) by \( \text{diag}(b_1, \ldots, b_n) \).

For a subring \( R \) of \( F \) containing \( \mathfrak{o} \), we denote the set of symmetric square matrices of degree \( n \) with entries in \( R \) by \( \text{Sym}_n(R) \). We say \( B = (b_{ij}) \in \text{Sym}_n(F) \) is half-integral if \( 2b_{ij} \in \mathfrak{o} \), and \( b_{ii} \in \mathfrak{o} \) for any \( i, j \) and denote the set of non-degenerate half-integral symmetric matrix of degree \( n \) by \( \mathcal{H}_n(\mathfrak{o})^{nd} \). For \( B \in \mathcal{H}_n(\mathfrak{o})^{nd} \), we write \( \text{deg}(B) = n \).
When there exists $U \in \text{GL}_n(R)$ such that $B' = U^t B U$ for $B, B' \in \mathcal{H}_n(o)^{\text{nd}}$, we say they are $R$-equivalent and write $B \sim_R B'$.

For $a \in F^\times$, let $F(a^{1/2})$ be the field extension of $F$ obtained by adjoining $a^{1/2}$. We define $\chi(a) = 1, -1, 0$ if $F(a^{1/2})$ is $F$, an unramified quadratic extension of $F$, or a ramified extension of $F$, respectively. More concretely, let $a = p^r c \in F^\times$ with $r = \text{ord}(a)$ and $c \in o^\times$. Then $\chi(a) = \left( \frac{c}{p} \right)$ if $r \equiv 0 \text{ mod } 2$, and 0 otherwise when $p$ is odd, and

$$
\chi(a) = \begin{cases} 
1 & \text{if } r \equiv 0 \text{ mod } 2, c \equiv 1 \text{ mod } 8 \\
-1 & \text{if } r \equiv 0 \text{ mod } 2, c \equiv 5 \text{ mod } 8 \\
0 & \text{otherwise}
\end{cases}
$$

when $p = 2$.

Let $B \in \mathcal{H}_n(o)^{\text{nd}}$. We define

$$
\Delta_B = \begin{cases} 
\text{ord(det } B) + n - 1 & \text{if } n \text{ is odd} \\
\text{ord(det } B) + n - 2 & \text{if } n \text{ is even, and ord(det } B) \text{ is odd} \\
\text{ord(det } B) + n - 1 & \text{if } n \text{ is even, ord(det } B) \text{ is even, and } \xi_B = 0 \\
\text{ord(det } B) + n & \text{if } n \text{ is even, ord(det } B) \text{ is even, and } \xi_B \neq 0,
\end{cases}
$$

where $\xi_B = \chi((-1)^{n/2} \text{det } B)$, which is defined only when $n$ is even, and also set

$$
\varepsilon_B = \begin{cases} 
\Delta_B & \text{if } n \text{ is odd} \\
\Delta_B - 1 + \xi_B^2 & \text{if } n \text{ is even.}
\end{cases}
$$

Finally, if $B$ is $F$-equivalent to $\text{diag}(b_1, \ldots, b_n)$, then we put

$$
\varepsilon_B = \prod_{i<j} (b_i, b_j)
$$

and

$$
\eta_B = (-1, -1)^{\lfloor (n+1)/4 \rfloor} (-1, \text{det } B)^{\lfloor (n-1)/2 \rfloor} \varepsilon_B.
$$

Note that $\varepsilon_B$ does not depend on the choice of $b_1, \ldots, b_n$. Here $(\cdot, \cdot)$ denotes the Hilbert symbol [Cas78, Section 3.2], and $\lfloor \cdot \rfloor$ the floor function.

1.2. Gross-Keating invariants.

**Definition 1.1.** Let $B = (b_{ij}) \in \mathcal{H}_n(o)^{\text{nd}}$. Let $S(B)$ be the set of all non-decreasing sequences $(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0}^n$ such that

$$
\text{ord}(b_{ii}) \geq a_i \quad (1 \leq i \leq n),
$$

$$
\text{ord}(2b_{ij}) \geq (a_i + a_j)/2 \quad (1 \leq i, j \leq n),
$$

then we put

$$
\varepsilon_B = \prod_{i<j} (b_i, b_j)
$$

and

$$
\eta_B = (-1, -1)^{\lfloor (n+1)/4 \rfloor} (-1, \text{det } B)^{\lfloor (n-1)/2 \rfloor} \varepsilon_B.
$$
and \( S(B) := \bigcup_{U \in \text{GL}_n(o)} S(U^tBU) \). The Gross-Keating invariant \(\text{GK}(B) = (a_1, \ldots, a_n)\) of \( B \) is defined by

\[
\begin{align*}
  a_1 &= \max_{y_1 \in S(B)} y_1, \\
  a_2 &= \max_{(a_1, y_2, \ldots) \in S(B)} y_2, \\
  \vdots \\
  a_n &= \max_{(a_1, a_2, \ldots, a_{n-1}, y_n) \in S(B)} y_n.
\end{align*}
\]

By definition \(\text{GK}(B)\) only depends on the \(o\)-equivalence class of \( B \), but obviously the definition is not very useful for computing \(\text{GK}(B)\).

Now we review a procedure to compute the Gross-Keating invariant of \( B \). When \( p \) is odd, it is well-known that \( B \) is \( o \)-equivalent to a diagonal matrix; we will review an algorithm to find such a diagonal matrix in Subsection 2.1.

**Theorem 1.2.** [IK15, Proposition 6.1] Let \( p \) be odd, and \( B = \text{diag}(t_1, \ldots, t_n) \) such that \( \text{ord}(t_1) \leq \text{ord}(t_2) \leq \cdots \leq \text{ord}(t_n) \). Then \(\text{GK}(B) = (a_1, \ldots, a_n)\), where \( a_i = \text{ord}(t_i) \).

**Example 1.3.** Let \( B = \begin{pmatrix} 20 & 24 & 11 \\ 11 & 12 & 8 \end{pmatrix} \in \mathcal{H}_3(\mathbb{Z}_3) \).

We can calculate \(\text{GK}(B)\) using our program as follows:

\[
\text{In}[1] := \text{computeGK}\left[\{\{20, 24, 11\}, \{24, 96, 12\}, \{11, 12, 8\}\}\right], 3
\]

\[
\text{Out}[1] = \{0, 1, 3\}
\]

Internally, it finds the equivalent diagonal matrix \(\text{diag}(2 \cdot 3^0, 1 \cdot 3^2, 2 \cdot 3^3)\) by:

\[
\text{In}[2] := \text{reduceJordanZp}\left[\{\{20, 24, 11\}, \{24, 96, 12\}, \{11, 12, 8\}\}\right], 3
\]

\[
\text{Out}[2] = \text{FJC}\left[\{0, 2\}, \{1, 2\}, \{3, 2\}\right]
\]

\(\text{FJC}\) is one of the data types used in \(\text{computeGK}\) to represent the Jordan components of a matrix, and \(\text{FJC}\) means the ‘flattened version’ of \(\text{JC}\), which is another data type of the same kind; see Example 1.6 for the use of \(\text{JC}\). You can represent \(\text{diag}(u_1p^{e_1}, \ldots, u_np^{e_n})\) with \( u_i \in \{1, \ldots, p-1\} \) and \( e_i \in \mathbb{Z}_{\geq 0} \) by \(\text{FJC}\) with arguments \(\{u_1, e_1\}, \ldots, \{u_n, e_n\}\).

For the rest of this subsection, we assume that \( p = 2 \). As usual in the study of quadratic forms, the story becomes more complicated. To obtain the Gross-Keating invariant and other related quantities for a given half-integral matrix, we need to undergo several reduction procedures. Let \( H = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \) and \( Y = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \).

**Definition 1.4.** Let \( \Sigma = \{(1), (3), (5), (7), H, Y\} \). We define \(\mathcal{C}\) as the set of finite sequences \(\beta = \{(k_i, C_i)\}_{i=1}^r\) of pairs \((k_i, C_i)\) with \( k_i \in \mathbb{Z}_{\geq 0} \) and \( C_i \) is a matrix obtained as an orthogonal sum of elements of \(\Sigma\). Define \(\Omega_D\) as the set of elements of the form
(\(u_1\)) or \((u_1) \perp (u_2)\) with \(u_i \in \{1,3,5,7\}\). Let \(\Omega_{E} := \{H,Y\}\) and \(\Omega := \Omega_D \cup \Omega_{E}\). We define \(\mathcal{J}C_s := \{\beta \in \mathcal{J}C : \beta = \{(k_i,C_i)\}_{i=1}^{r} \text{ with } C_i \in \Omega \text{ for all } i\}\).

For \(\beta = \{(k_i,C_i)\}_{i=1}^{r} \in \mathcal{J}C\), we define \([\beta] := 2^{k_1}C_1 \perp \cdots \perp 2^{k_r}C_r\). We say two elements of \(\mathcal{J}C\) are equivalent if the corresponding matrices are \(o\)-equivalent. We define \(\deg \beta, \det \beta, \epsilon_\beta, \xi_\beta\), and \(\eta_\beta\) as the corresponding quantities for the matrix \([\beta]\). For a positive integer \(1 \leq j \leq r\), we set \(\beta^{[j]} := \{(k_i,C_i)\}_{i=1}^{j} \in \mathcal{J}C\).

The following is \(\text{[CIKY17, Definition 2.1]}\), suitably adapted to \(\mathcal{J}C\).

**Definition 1.5.** We call \(\beta = \{(k_i,C_i)\}_{i=1}^{r} \in \mathcal{J}C_s\) a weak canonical form if it satisfies the following conditions:

(i) We have \(k_1 \leq \cdots \leq k_r\).

(ii) If \(C_i\) is diagonal, then \(k_i < k_{i+1}\) and for any \(j \leq i - 1\) such that \(k_j = k_i\), \(C_j\) is either \(H\) or \(Y\).

(iii) If \(C_{i+1}\) and \(C_j\) with \(j \leq i\) are diagonal such that \(k_{i+1} = k_j + 1\), and that \(\deg \beta^{[i]}\) are even, then \(\xi_{\beta^{[i]}} = 0\).

When a matrix \(B \in \mathcal{H}_n(o)^{\text{nd}}\) is given, we can find \(\beta \in \mathcal{J}C_s\) such that \([\beta] \sim_{Z_2} B\) using Watson reduction as explained in Subsection 2.2. Then we can convert it to an equivalent weak canonical form \(\beta'\); see Subsection 2.3 for an algorithm. These reduction procedures are implemented in \(\text{computeGK}\).

**Example 1.6.** Let \(B = \begin{pmatrix} 3 & 0 & 132 \\ 0 & 81 & 0 \\ 132 & 0 & 5822 \end{pmatrix} \in \mathcal{H}_3(Z_2)^{\text{nd}}\). This is \(o\)-equivalent to a diagonal matrix:

\[
\begin{align*}
\text{In[3]} &= \text{reduceJordanZp[}\{\{3,0,132\},\{0,81,0\},\{132,0,5822\}\}\text{,2]} \\
\text{Out[3]} &= \text{FJC[}\{0,3\},\{0,1\},\{1,7\}\text{]} \\
\text{In[4]} &= \text{reduceWatson[}\{\{3,0,132\},\{0,81,0\},\{132,0,5822\}\}\text{]} \\
\text{Out[5]} &= \text{JC[}\{0,\{1,3\}\},\{1,\{7\}\}\text{]} \\
\text{This gives } \beta = \{\{0,(1) \perp (3)\},\{1,(7)\}\}, \text{ which is not a weak canonical form.} \\
\text{In[6]} &= \text{checkWeakCanonicalFormQ[JC[}\{0,\{1,3\}\},\{1,\{7\}\}\text{]}\text{]} \\
\text{Out[6]} &= \text{False}
\end{align*}
\]

Let us find a weak canonical form \(\{(0,(1) \perp (1)),(1,(5))\}\) equivalent to \(\beta\) as follows:

\[
\begin{align*}
\text{In[7]} &= \text{reduceWeakCanonical[JC[}\{0,\{1,3\}\},\{1,\{7\}\}\text{]}\text{]} \\
\text{Out[7]} &= \text{JC[}\{0,\{1,1\}\},\{1,\{5\}\}\text{]}
\end{align*}
\]

We can do a double check:
We say that \( k \) or equal to the maximum of \( k_i \), put
\[
\mathcal{D}_m = \{ 1 \leq j \leq r \mid k_j = m \text{ and } C_j \in \Omega_D \},
\]
and
\[
\mathcal{E}_m = \{ 1 \leq j \leq r \mid k_j = m \text{ and } C_j \in \Omega_E \}.
\]
We say that \( \beta \) is pre-optimal if it satisfies the following conditions:

(i) For any \( m \), \( \sum_{j \in \mathcal{D}_m} \deg C_j \leq 2 \) and there are integers \( 1 \leq i \leq j \) such that \( \mathcal{E}_m = \{ i, i+1, \ldots, j-1 \} \). If \( i = j \), we simply put \( \mathcal{E}_m = \phi \).

(ii) Let \( 1 \leq i < j \leq r \).
   (a) If \( i \in \mathcal{D}_{m_1} \) and \( j \in \mathcal{D}_{m_2} \), then \( m_1 \leq m_2 \).
   (b) If \( i \in \mathcal{E}_{m_1} \) and \( j \in \mathcal{E}_{m_2} \), then \( m_1 \leq m_2 \).
   (c) If \( i \in \mathcal{D}_{m_1} \) and \( j \in \mathcal{E}_{m_2} \), then \( m_1 \leq m_2 - 1 \).
   (d) If \( i \in \mathcal{E}_{m_1} \) and \( j \in \mathcal{D}_{m_2} \), then \( m_1 \leq m_2 + 1 \).

(iii) Suppose that \( C_i \in \Omega_D \) with \( \deg C_i = 2 \). Then \( i \geq 2 \) and one of the following conditions hold:
   (a) \( \deg \beta[i] \) is even and \( \xi_{\beta[i-1]} = \xi_{\beta[i]} = 0 \).
   (b) \( \deg \beta[i] \) is odd and \( \text{ord}(\text{det} \beta[i-1]) + k_i \) is even.

(iv) Suppose that \( C_i \in \Omega_D, C_{i-1} \in \Omega_E \), and that \( k_i = k_{i-1} - 1 \). If \( \deg C_i \neq 2 \), then one of the following conditions holds:
   (a) \( \deg \beta[i] \) is even and \( \text{ord}(\text{det} \beta[i]) \) is even.
   (b) \( \deg \beta[i] \) is odd and \( \xi_{\beta[i-1]} = 0 \).

(v) Suppose that \( C_i \in \Omega_D, C_{i+1} \in \Omega_E \), and that \( k_i = k_{i+1} - 1 \). Then \( \deg C_i = 1 \), and one of the following conditions holds:
   (a) \( \deg \beta[i] \) is even and \( \text{ord}(\text{det} \beta[i]) \) is odd.
   (b) \( \deg \beta[i] \) is odd and \( \xi_{\beta[i-1]} \neq 0 \) if \( i \geq 2 \).

(vi) Suppose that \( C_{i+1} \in \Omega_D \) and \( C_j \in \Omega_D \) with \( j \leq i, k_{i+1} = k_j + 1 \), and \( \deg \beta[i] \) is even. Then \( \xi_{\beta[i]} = 0 \).

There is an algorithm \[CIKY17\] Proposition 2.1 to obtain an equivalent pre-optimal form from a weak canonical form, and our program has an implementation of it. Since its complete statement occupies more than one page, we refer the reader to the original article. Instead, we give an example.

**Example 1.8.** Consider the weak canonical form \( \{(0, (1) \perp (1)), (1, (5))\} \) of Example 1.6, which is not a pre-optimal form.

\[
\text{In}[9]:= \text{checkPreOptimalFormQ[JJC[\{0, \{1, 1\}\}, \{1, \{5\}\}]]}
\]

\[
\text{Out}[9]=\text{True}
\]
We can get an equivalent pre-optimal form as follows:

```math
In[10]:= reducePreOptimal[JC[{0, {1, 1}, {1, 5}}]]
Out[10]= JC[{0, {1}}, {0, {1}}, {1, 5}]
```

```math
In[11]:= checkPreOptimalFormQ[JC[{0, {1}}, {0, {1}}, {1, 5}]]
Out[11]= True
```

This example demonstrates why we need to distinguish

\((0, (1) \perp (1)), (1, (5))\)

from

\((0, (1)), (0, (1)), (1, (5))\)

although they give the same diagonal matrix. This is the reason we define the notion of weak canonical forms and pre-optimal forms for the elements of \( \mathbb{J} \mathbb{C} \) not matrices.

With a pre-optimal form, we can obtain the Gross-Keating invariant of the corresponding matrix; see Subsection 1.5 for a different method.

**Theorem 1.9.** \([\text{CIKY17, Theorem 3.1}]\) Let \( \beta = \{(k_i, C_i)\}_{i=1}^r \) be a pre-optimal form of degree \( n \). Then \( \text{GK}(\beta) = (a_1, \ldots, a_n) \) is given as follows: For each \( 1 \leq s \leq r \), put \( \bar{n}_s = \deg C_1 + \cdots + \deg C_s \) and

(i) If \( C_s \in \Omega_E \), then \( (a_{\bar{n}_s-1}, a_{\bar{n}_s}) = (k_s, k_s) \).

(ii) Assume that \( C_s \in \Omega_D \) and \( \deg C_s = 1 \).

(a) If \( \bar{n}_s \) is odd, then

\[
a_{\bar{n}_s} = \begin{cases} 
    k_s + 2 & \text{if } \text{ord}(\det \beta^{[s-1]}) \text{ is odd} \\
    k_s + 1 & \text{if } \text{ord}(\det \beta^{[s-1]}) \text{ is even and } \xi_{\beta^{[s-1]}} = 0 \\
    k_s & \text{if } \xi_{\beta^{[s-1]}} \neq 0,
\end{cases}
\]

where we make the convention that \( \text{ord}(\det \beta^{[0]}) = 0 \) and \( \xi_{\beta^{[0]}} = 1 \).

(b) If \( \bar{n}_s \) is even, then

\[
a_{\bar{n}_s} = \begin{cases} 
    k_s & \text{if } \text{ord}(\det \beta^{[s]}) \text{ is odd} \\
    k_s + 1 & \text{if } \text{ord}(\det \beta^{[s]}) \text{ is even and } \xi_{\beta^{[s]}} = 0 \\
    k_s + 2 & \text{if } \xi_{\beta^{[s]}} \neq 0.
\end{cases}
\]

(iii) If \( C_s \in \Omega_D \) and \( \deg C_s = 2 \), then \( (a_{\bar{n}_s-1}, a_{\bar{n}_s}) = (k_s + 1, k_s + 1) \).

**Example 1.10.** Let us resume our computation from Example 1.8. We can compute the Gross-Keating invariant from the pre-optimal form \( \{(0, (1)), (0, (1)), (1, (5))\} \) as follows:

```math
In[12]:= computeGK[JC[{0, {1}}, {0, {1}}, {1, 5}]], 2]
Out[12]= \{0, 1, 2\}
```

We can also use our original matrix \( B \) from Example 1.6 as input, and the program goes through the necessary reductions internally.
1.3. Naive extended Gross-Keating datum.

Definition 1.11. An element $H = (a_1, \ldots, a_n; \varepsilon_1, \ldots, \varepsilon_n)$ of $\mathbb{Z}_{\geq 0}^n \times \{-1, 0, 1\}^n$ is a naive extended Gross-Keating (EGK) datum of length $n$ if the following conditions hold:

(i) $a_1 \leq \cdots \leq a_n$.

(ii) Suppose that $i$ is even. Then $\varepsilon_i \neq 0$ if and only if $a_1 + \cdots + a_i$ is even.

(iii) If $i$ is odd, then $\varepsilon_i \neq 0$.

(iv) $\varepsilon_1 = 1$.

(v) If $i \geq 3$ is odd and $a_1 + \cdots + a_{i-1}$ is even, then $\varepsilon_i = \varepsilon_{i-2} a_i + a_{i-1}$.

Let us define a naive EGK datum $H = (a_1, \ldots, a_n; \varepsilon_1, \ldots, \varepsilon_n)$ of $B \in \mathcal{H}_n(\mathfrak{o})^{\text{nd}}$. First, each $a_i$ is given by $\text{GK}(B) = (a_1, \ldots, a_n)$.

Let $p$ be odd and assume that $B$ is $\mathbb{Z}_p$-equivalent to $\text{diag}(t_1, \ldots, t_n)$ such that $\text{ord}(t_1) \leq \text{ord}(t_2) \leq \cdots \leq \text{ord}(t_n)$. Following [IK15, Proposition 6.1], let

\[
\varepsilon_i = \begin{cases} 
\xi_{B[i]} & \text{if } i \text{ is even}, \\
\eta_{B[i]} & \text{if } i \text{ is odd,}
\end{cases}
\]

where $B[i] = \text{diag}(t_1, \ldots, t_i)$.

Let $p = 2$ and assume that $B$ is $\mathbb{Z}_2$-equivalent to $[\beta]$, where $\beta = \{(k_i, C_i)\}_{i=1}^r$ is a pre-optimal form with $n_i = \deg C_i$. As in [CIKY17, Theorem 4.3], let

\[
\varepsilon_i = \begin{cases} 
1 & \text{if } i = 1 \\
\xi_{\beta[i]} & \text{if } i \text{ is even and } i = \deg \beta[i] \text{ for some } s \\
\eta_{\beta[i]} & \text{if } i \geq 3 \text{ is odd and } i = \deg \beta[i] \text{ for some } s \\
\eta_{\beta[i]} \xi_{\beta[i]} & \text{if } i \geq 3 \text{ is odd, } i = \deg \beta[i] - 1 \text{ for some } s \text{ such that } n_s = 2, \\
al + 1 + a_i + a_{i+1} \text{ is even} & \\
0 & \text{if } i \text{ is even, } i = \deg \beta[i] - 1 \text{ for some } s \text{ such that } n_s = 2, \text{ and } a_1 + \cdots + a_i \text{ is odd} \\
\pm 1 & \text{if } i = \deg \beta[i] - 1 \geq 2 \text{ for some } s \text{ such that } n_s = 2, \text{ and } i + 1 + a_1 + \cdots + a_{\lfloor i+1/2 \rfloor} \text{ is odd.}
\end{cases}
\]

Using computeGK, we can find a naive EGK datum of elements of $\mathcal{H}_n(\mathfrak{o})^{\text{nd}}$.

Example 1.12. Consider $B \in \mathcal{H}_3(\mathbb{Z}_{3})^{\text{nd}}$ from Example 1.3. A naive EGK datum of $B$ can be found as follows:

\[
\begin{align*}
\text{In}[13] := & \quad \text{computeGK}([\{3,0,132\}, \{0,81,0\}, \{132,0,5822\}], 2) \\
\text{Out}[13] := & \quad \{0,1,2\}
\end{align*}
\]

\[
\begin{align*}
\text{In}[14] := & \quad \text{computeNEGKdatum}([\{20,24,11\}, \{24,96,12\}, \{11,12,8\}], 3) \\
\text{Out}[14] := & \quad \{\{0,1,3\}, \{1,0,-1\}\}
\end{align*}
\]
We can also check if the output satisfies the conditions of Definition 1.11:

\[
\text{In[15]:= checkNEGKdatumQ[{{0,1,3},{1,0,-1}}]}
\]

\[
\text{Out[15]= True}
\]

**Example 1.13.** Let \( B \in \mathcal{H}_3(\mathbb{Z}_2) \) nd from Example 1.6. We can get a naive EGK datum of \( B \):

\[
\text{In[16]:= computeNEGKdatum[{{3,0,132},{0,81,0},{132,0,5822}},2]}
\]

\[
\text{Out[16]= {{0,1,2},{1,0,-1}}}
\]

The same result can be obtained using the pre-optimal form in Example 1.8:

\[
\text{In[17]:= computeNEGKdatum[JC[{0,1},{0,1},{1,5}],2]}
\]

\[
\text{Out[17]= {{0,1,2},{1,0,-1}}}
\]

Again, we can check if the output is a naive EGK datum:

\[
\text{In[18]:= checkNEGKdatumQ[{{0,1,2},{1,0,-1}}]}
\]

\[
\text{Out[18]= True}
\]

A naive EGK datum \( H \) of \( B \) is not an invariant of the \( o \)-equivalence class of \( B \). It is not even uniquely defined as one can see from the last entry of (1.2). However, there is an easy way to get an invariant from \( H \), which is called the extended Gross-Keating datum of \( B \), denoted by \( \text{EGK}(B) \); see [CIKY17, Section 4]. Since a naive EGK datum is sufficient for most of our purposes, we have no instruction in \( \text{computeGK} \) to compute \( \text{EGK}(B) \).

### 1.4. Siegel series

Let \( B \in \mathcal{H}_n(o) \) nd. We consider the problem of computing the Siegel series of \( B \) and closely related functions.

**Definition 1.14.** Let \( \psi(a) = \exp(2\pi \sqrt{-1} \tilde{a}) \), where \( \tilde{a} \in \mathbb{Q} \) such that \( \tilde{a} - a \in o \) for \( a \in F \). For \( B \in \mathcal{H}_n(o) \) nd, the (local) Siegel series \( b(B,s) \) is defined by

\[
b(B,s) = \sum_{R \in \text{Sym}_n(F)/\text{Sym}_n(o)} \psi(\text{tr}(BR)) \mu(R)^{-s},
\]

where \( \mu(R) = [R o^n + o^n : o^n] \).

Define a polynomial \( \gamma(B;X) \) in \( X \) by

\[
\gamma(B;X) = \begin{cases} 
(1 - X) \prod_{i=1}^{n/2} (1 - p^{2i} X^2)^2 (1 - p^{n/2} \xi_B X)^{-1} & \text{if } n \text{ is even} \\
(1 - X) \prod_{i=1}^{(n-1)/2} (1 - p^{2i} X^2) & \text{if } n \text{ is odd}
\end{cases}
\]

It is known that there exists a polynomial \( F(B;X) \in \mathbb{Z}[X] \) such that

\[
b(B,s) = \gamma(B;p^{-s}) F(B;p^{-s}).
\]
Fix an indeterminate $X^{1/2}$ such that $(X^{1/2})^2 = X$. We define a Laurent polynomial $	ilde{F}(B; X)$ in $X^{1/2}$ as

\[(1.3) \quad \tilde{F}(B; X) := X^{-\epsilon n/2} F(B; p^{-(n+1)/2} X). \]

Let us explain how to find $F(B; X)$ with a naive EGK datum of $B$.

**Definition 1.15.** For $e, \tilde{e} \in \mathbb{Z}$ and $\xi \in \{-1, 0, 1\}$, we define rational functions $C(e, \tilde{e}, \xi; X)$ and $D(e, \tilde{e}, \xi; X)$ in $X^{1/2}$ by

\[ C(e, \tilde{e}, \xi; X) = \frac{p^{\tilde{e}/4} X^{-(e-\tilde{e})/2-1}(1 - \xi p^{-1/2} X)}{X^{-1} - X} \]

and

\[ D(e, \tilde{e}, \xi; X) = \frac{p^{\tilde{e}/4} X^{-(e-\tilde{e})/2}}{1 - \xi X}. \]

Let

\[(1.4) \quad C_i(e, \tilde{e}, \xi; X) = \begin{cases} C(e, \tilde{e}, \xi; X) & \text{if } i \in \mathbb{Z} \text{ is even} \\ D(e, \tilde{e}, \xi; X) & \text{if } i \in \mathbb{Z} \text{ is odd.} \end{cases} \]

**Definition 1.16.** For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_\geq 0^n$ and an integer $1 \leq i \leq n$, define $\mathbf{e}_i = \mathbf{e}_i(\mathbf{a})$ as

\[ \mathbf{e}_i = \begin{cases} a_1 + \cdots + a_i & \text{if } i \text{ is odd} \\ 2\lfloor (a_1 + \cdots + a_i)/2 \rfloor & \text{if } i \text{ is even.} \end{cases} \]

For a naive EGK datum $H = (a_1, \ldots, a_n; \varepsilon_1, \ldots, \varepsilon_n)$ we define a rational function $\mathcal{F}(H; X)$ in $X^{1/2}$ as follows: for the naive EGK datum $H = (; ;)$ of length zero we set $\mathcal{F}(H; X) = 1$. Now suppose that $n \geq 1$. Then $H' = (a_1, \ldots, a_{n-1}; \varepsilon_1, \ldots, \varepsilon_{n-1})$ is a naive EGK datum of length $n - 1$. We define $\mathcal{F}(H; X)$ recursively by

\[(1.5) \quad \mathcal{F}(H; X) = C_n(\mathbf{e}_n, \mathbf{e}_{n-1}, \xi; X) \mathcal{F}(H'; p^{1/2} X) + \zeta C_n(\mathbf{e}_n, \mathbf{e}_{n-1}, \xi; X^{-1}) \mathcal{F}(H'; p^{1/2} X^{-1}), \]

where $\xi = \varepsilon_n$ or $\varepsilon_{n-1}$ according as $n$ is even or odd, and $\zeta = 1$ or $\varepsilon_n$ according as $n$ is even or odd. We put $\varepsilon_0 = 0$ and $\varepsilon_0 = 1$.

**Remark 1.17.** In [CIKY17], the initial condition for $\mathcal{F}(H; X)$ is given by

\[ \mathcal{F}(H; X) = X^{-a_1/2} + X^{-a_1/2 + 1} + \cdots + X^{a_1/2 - 1} + X^{a_1/2} \]

for $H = (a_1, \varepsilon_1)$ of length 1. This agrees with our treatment of $\mathcal{F}$.

**Theorem 1.18.** [CIKY17, Theorem 5.5] Let $B \in \mathcal{H}_n(\mathfrak{a})^{nd}$ and $H$ be a naive EGK datum of $B$ as in (1.1) and (1.2). Then we have

\[ \tilde{F}(B; X) = \mathcal{F}(H; X). \]
This theorem allows us to use (1.5) to obtain \( F(B; X) \) once a naive EGK datum \( H \) of \( B \) is known. Note that \( \varepsilon_i \neq 0 \) for \( i \) odd in Definition 1.11. Hence, \( \zeta \) in (1.5) is 1 or \(-1\), which implies the following functional equation

\[
F(H; X) = \zeta F(H; X^{-1}).
\]

By incorporating this, we can slightly modify (1.5) into the following for \( m \):

\[
(1.6) \quad F(H; X) = C_n(e, e_{n-1}, \xi; X) F(H'; p^{1/2} X) + \xi' C_n(e, e_{n-1}, \xi; X^{-1}) F(H''; p^{-1/2} X),
\]

where \( \xi' = \varepsilon_{n-1} \) if \( n \) is even, or \( \varepsilon_n \) if \( n \) odd. Instead of calculating \( F(H; X) \) as a rational function with irrational coefficients, we may tabulate the values \( F(H'; p^l X) \) with \( l \in \mathbb{Z}_{\geq 0} \) recursively using (1.6). Since \( F(B; X) \) is a polynomial of degree \( e_B \) with integer coefficients, \( F(B; p^k) \) with \( k \in \mathbb{Z}_{\geq 0} \) must be an integer, and then an interpolation is feasible. By rewriting (1.3), we have

\[
F(B; X) = (X p^{(n+1)/2})^{e_B/2} F(H; X p^{(n+1)/2}),
\]

and hence,

\[
(1.7) \quad F(B; p^k) = (p^{k+(n+1)/2})^{e_B/2} F(H; p^{2k+n+1}) \in \mathbb{Z}
\]

by setting \( X = p^k, \ k \in \mathbb{Z}_{\geq 0} \). When using (1.6) for this purpose, we need some care to avoid evaluating \( C_i(e, \xi; X) \) in (1.4) at \( X = 1 \) since it may have a pole there. When \( n = 1 \), it is safe to use (1.6) for \( X = p^{l/2} \) with \( l \geq 1 \). When \( n = 2 \), it is so for \( X = p^{l/2} \) with \( l \geq 2 \). In general, we can calculate the values at \( X = p^{l/2} \) with \( l \geq n \). Thus, there is no problem in finding the values of the right-hand side of (1.7) at \( k = 0, \ldots, e_B \), which is enough to fix \( F(B; X) \) and in turn, \( \tilde{F}(B; X) \).

**Example 1.19.** Let \( B \in \mathcal{H}_3(\mathbb{Z}_2) \) from Example 1.6. Then \( F(B; X) \) is obtained with

\[
\text{In}[19]:= \quad \text{computeFpoly}[[\{3,0,132\},\{0,81,0\},\{132,0,5822\}],[2,X]]
\]

\[
\text{Out}[19]= \quad 1-64 \ X^3
\]

We can also use the pre-optimal form we found as an input to achieve the same result :

\[
\text{In}[20]:= \quad \text{computeFpoly}[JC[\{0,\{1\}\},\{0,\{1\}\},\{1,\{5\}\}],2,X]
\]

\[
\text{Out}[20]= \quad 1-64 \ X^3
\]

We can do the same thing for odd prime \( p \).

**Example 1.20.** Consider \( B \in \mathcal{H}_3(\mathbb{Z}_3) \) in Example 1.3. We can calculate \( F(B; X) \) as above :

\[
\text{In}[21]:= \quad \text{computeFpoly}[[\{20,24,11\},\{24,96,12\},\{11,12,8\}],[3,X]]
\]

\[
\text{Out}[21]= \quad 1-6561 \ X^4
\]
1.5. **Reliability checks.** There are several ways to check the reliability of \texttt{computeGK}. As we saw in the examples, we can use the following pairs of commands to test for self-consistency.

- \texttt{reduceWeakCanonical - checkWeakCanonicalFormQ};
- \texttt{reducePreOptimal - checkPreOptimalFormQ};
- \texttt{computeNEGKdatum - checkNEGKdatumQ}.

Let \( B \in \mathcal{H}_n(o) \) and \( \text{GK}(B) = (a_1, \ldots, a_n) \). Then [IK15, Theorem 0.1] says

\[
\Delta_B = a_1 + \cdots + a_n.
\]

This is also useful to check the validity of the Gross-Keating invariant obtained. If we are interested in finding \( \text{GK}(B) \) only, it is not necessary to find a pre-optimal form \( \beta \in \mathcal{J}_C \) such that \( B \sim_{\mathbb{Z}_2} [\beta] \). In fact, Watson reduction (Subsection 2.2) is sufficient; see [CY18] for details. This method also has been used to test if these two methods produce the same results, and we have obtained the agreement for thousands of randomly generated matrices.

Regarding \( F(B; X) \), there are several facts that we may employ for checks:

- it is a polynomial with integer coefficients, of degree \( e_B \), and \( F(B; 0) = 1 \);
- it satisfies the following relation

\[
F(B; p^{-n-1}X^{-1}) = \zeta \times (p^{(n+1)/2}X)^{-\epsilon_B} F(B; X),
\]

where \( \zeta = 1 \) or \( \epsilon_n \) depending on whether \( n \) is even or odd.

The command \texttt{checkFpolyDual} in our program checks the latter.

There is a different computer code to obtain \( F(B; X) \), which is publicly available. King’s LISP code [Kin03] and its recent extension by King, Poor, Shurman, and Yuen in [KPSY18] computes \( F(B; X) \) using the genus symbol of \( B \). This is based on the recursive formula in [Kat99], which is more complicated than (1.5). We compared the results for \( F(B; X) \) obtained by \texttt{computeGK} with those of King’s code for thousands of diagonal matrices \( B \) of various sizes and obtained the agreement. We add the remark that our approach based on (1.7), which uses the irrational numbers in the middle of the interpolation, could be actually slower than the other, which uses only integer arithmetic.

**Remark 1.21.** Watson reduction is sufficient to compute the Siegel series using the formula in [Kat99].

2. **Matrix reductions**

2.1. **Jordan decomposition.** Let \( p \) be any prime and \( B \in \mathcal{H}_n(o) \). Let us review how to find an orthogonal sum \( B' \) of Jordan components such that \( B \sim o B' \). By a Jordan component, we simply mean a matrix of degree 1, or a matrix of the form \( (b_{ij}) \in \mathcal{H}_2(\mathbb{Z}_2) \) such that \( \text{ord}(b_{11}), \text{ord}(b_{22}) > \text{ord}(b_{12}) \) when \( p = 2 \). We call an
orthogonal sum of the matrices of the latter form is of type II. Although this is a well-known result, it still requires some work to convert the steps described in the literature (for example, [Wat60, Cas78]) into an explicit algorithm. We have included a simple procedure for completeness, which we learned from the code used in [KPSY18].

Let $B = (b_{ij})_{1 \leq i,j \leq n}$ be given.

**Step 0**: By rearranging the rows and columns of $B$, we can assume that $B$ has an entry in the first row which has minimum valuation among all $b_{ij}$. Let $j_0$ be the smallest index among $1 \leq j \leq n$ such that $b_{ij}$ has minimal valuation.

**Step 1**: If $j_0 = 1$, then skip Step 2 and proceed to Step 3. If $j_0 \geq 3$, we can move $b_{1j_0}$ to the second column by swapping the rows and columns of $B$. Hence, we can assume that $j_0 = 2$, i.e., $b_{12}$ has minimum valuation among all $b_{ij}$. Note that $j_0$ could not be 1 by doing this since such an operation preserves the set of diagonal (and non-diagonal).

**Step 2**: This step is only necessary if $p$ is odd. Let $U = E_{12}(1)$, where $E_{ij}(a) \in \text{GL}_n(\mathfrak{o})$ with $a \in \mathfrak{o}$ denotes the matrix whose diagonal entries are 1 and the only non-zero non-diagonal entry is $a$ at the position $(i,j)$. Then $B' = (b'_{ij})$ defined by $B' = UBU^t$ has entries $b'_{11} = b_{11} + 2b_{12} + b_{22}$, $b'_{1j} = b_{1j} + b_{2j}$, $b'_{ij} = b_{ij}$ ($j > 1$), and $b'_{ij} = b_{ij}$ in other cases. Then $\text{ord}(b'_{11}) = \text{ord}(b_{12})$ and $\text{ord}(b'_{ij}) = \text{ord}(b_{ij}) \geq \text{ord}(b_{12} + b_{21}) = \text{ord}(b_{12})$ for $j > 1$. Therefore, $b'_{11}$ has minimum valuation among all $b'_{ij}$. Now we redefine $B$ as $B'$.

**Step 3**: Let $B_0 := (b_{11})$ if $b_{11}$ has minimum valuation, and $B_0 := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ otherwise, i.e. $b_{12}$ has minimum valuation with $\text{ord}(b_{11}) > \text{ord}(b_{12})$. Let $m = \text{deg} B_0 \in \{1, 2\}$. So $B$ takes the form

$$B = \begin{pmatrix} B_0 \\ X \\ B_1 \end{pmatrix}$$

for some $(n - m) \times m$ matrix $X$ and $B_1$ of degree $n - m$. Define a matrix of degree $n$ by

$$U = \begin{pmatrix} I_m \\ XB_0^{-1} \\ I_{n-m} \end{pmatrix}.$$ 

Now we claim that $U \in \text{GL}_n(\mathfrak{o})$. Note that $XB_0^{-1}$ has entries in $\mathfrak{o}$. Indeed, when $B_0$ has degree 1 this is due to the minimality of $\text{ord}(b_{11})$. When $\text{deg} B_0 = 2$, $c_{12} = -b_{12}(b_{11}b_{22} - b_{12}^2)^{-1}$ has minimum valuation $\text{ord}(c_{12}) = -\text{ord}(b_{12})$ among all entries of $B_0^{-1} = (c_{ij})$. Thus, $XB_0^{-1}$ has entries in $\mathfrak{o}$ in either case. Since $U$ is a lower triangular matrix with unit diagonal, its inverse also has entries in $\mathfrak{o}$. Hence, $U \in \text{GL}_n(\mathfrak{o})$.

We obtain

$$B' = UBU^t = \begin{pmatrix} B_0 \\ 0 \\ B'_1 \end{pmatrix}$$

with $B'_1 \in \mathcal{H}_{n-m}(\mathfrak{o})^{nd}$.

Repeating Steps 0-3 with matrices of smaller size, we eventually obtain a Jordan decomposition of $B$. The command `reduceJordanZp` follows this procedure.
Remark 2.1. To find an F-equivalent diagonal matrix, which is always possible even when \( p = 2 \), use the command reduceJordanK.

2.2. Watson reduction. Now assume that \( p = 2 \) and \( B \in \mathcal{H}_n(\mathbb{Z}_2) \) an orthogonal sum of the Jordan components. Then \( B \) is \( \mathbb{Z}_2 \)-equivalent to a matrix of the form

\[
2^{e_1}(V_1 \perp U_1) \perp \ldots \perp 2^{e_m}(V_m \perp U_m)
\]

with \( 0 \leq e_1 < \cdots < e_m \), \( U_i = \emptyset \) or \( u_1 \perp u_2 \) for \( u_1, u_2 \in \{1, 3, 5, 7\} \), and \( V_i = \emptyset \) or \( H \perp \cdots \perp H \perp Y \) (see, for instance, [Wat60, Theorem 35]). We say a matrix of the form (2.1) is Watson-reduced. Let us explain how to transform \( B \) into this form in an explicit manner. First note that a matrix (2.3) \((m_{ij})\) of the form repeatedly, we get (2.1) equivalent to (2.2).

Assume that \( B \) is of the form

\[
2^{e_i'}(V_i' \perp U_i') \perp \ldots \perp 2^{e_m'}(V_m' \perp U_m')
\]

as in (2.1), but \( U_i' = u_1 \perp \cdots \perp u_{k_i} \), not necessarily with \( 0 \leq k_i \leq 2 \), and

\[
V_i' = H \perp \ldots \perp Y \perp \ldots \perp H \perp \ldots \perp Y
\]

with \( m_i \geq 2 \) possibly.

To make a reduction into the form (2.1), we can use the following facts (see, for example, [Cas78, 118p.]): for any \( u_1, u_2, u_3 \in \{1, 3, 5, 7\} \), there exist \( u' \in \{1, 3, 5, 7\} \) and \( K \in \{H, Y\} \) such that

\[
(u_1) \perp (u_2) \perp (u_3) \sim_{\mathbb{Z}_2} (u') \perp 2K,
\]

and \( Y \perp Y \sim_{\mathbb{Z}_2} H \perp H \). See Table 2.2 for an explicit description of (2.3). Applying these rules repeatedly, we get (2.1) equivalent to (2.2).

| \((u_1, u_2, u_3)\) | \((u', K)\) | genus symbol | \((u_1, u_2, u_3)\) | \((u', K)\) | genus symbol |
|-------------------|-------------|--------------|-------------------|------------|--------------|
| \((1, 1, 1)\)     | \((3, Y)\)  | 13           | \((3, 3, 3)\)     | \((1, Y)\)  | 13           |
| \((1, 1, 3)\)     | \((5, H)\)  | 15           | \((3, 3, 5)\)     | \((3, H)\)  | 13           |
| \((1, 1, 5)\)     | \((7, Y)\)  | 17           | \((3, 3, 7)\)     | \((5, Y)\)  | 13           |
| \((1, 1, 7)\)     | \((1, H)\)  | 11           | \((3, 5, 5)\)     | \((5, H)\)  | 13           |
| \((1, 3, 3)\)     | \((7, H)\)  | 12           | \((3, 5, 7)\)     | \((7, H)\)  | 13           |
| \((1, 3, 5)\)     | \((1, H)\)  | 13           | \((3, 7, 7)\)     | \((1, Y)\)  | 13           |
| \((1, 3, 7)\)     | \((3, H)\)  | 13           | \((5, 5, 5)\)     | \((7, Y)\)  | 13           |
| \((1, 5, 5)\)     | \((3, Y)\)  | 13           | \((5, 5, 7)\)     | \((1, H)\)  | 13           |
| \((1, 5, 7)\)     | \((5, H)\)  | 13           | \((5, 7, 7)\)     | \((3, H)\)  | 13           |
| \((1, 7, 7)\)     | \((7, H)\)  | 13           | \((7, 7, 7)\)     | \((5, Y)\)  | 13           |

Table 1. \((u_1, u_2, u_3)\) and \((u', K)\) such that \((u_1) \perp (u_2) \perp (u_3) \sim_{\mathbb{Z}_2} (u') \perp 2K\)

Example 2.2. Use the command reduceWatson for this procedure.

\texttt{In[22]:= reduceWatson[JCE[\{0,\{1,1,1,1\}\},\{1,\{Y\}\}\}]}\n\texttt{Out[22]= JCE[\{0,\{5\}\},\{1,\{H,H,H\}\}\]}
2.3. **Weak canonical reduction.** Assume that $B$ is Watson-reduced, i.e. of the form \((2.1)\). We can easily find $\beta \in \mathbb{JC}_a$ such that $[\beta] \sim_{\mathbb{Z}_2} B$, and Conditions \((\iota)\) and \((\ii)\) of Definition 1.5 are met. We want to find a weak canonical form equivalent to $\beta$. Note that $\xi_{B'' \oplus 2^k K} \neq 0 \iff \xi_{B''} \neq 0$, and $\deg_{B'' \oplus 2^k K} = \deg_{B''} \pmod{2}$ for any $B'' \in H_a(\alpha)^{pd}$ and $k \in \mathbb{Z}_{\geq 0}$, where $K$ is either $H$ or $Y$. Hence, if $\beta'$ denotes the subsequence of $\beta$ obtained by removing all the elements of the form $(k_i, C_i)$ with $C_i \in \Omega_\epsilon$, then $\beta$ satisfies Condition \((\iii)\) of Definition 1.5 if and only if so does $\beta'$. Therefore, it is sufficient to find a weak canonical form $\beta''$ equivalent to $\beta'$.

Now we simply assume that $\beta = \{(k_i, C_i)\}_{i=1}^r \in \mathbb{JC}_a$ with $C_i \in \Omega_\Delta$. Suppose that it is not a weak canonical form but satisfies \((\iota)\) and \((\ii)\) of Definition 1.5.

Let $j \in \{1, \ldots, r - 1\}$ be the minimal position at which Condition \((\iii)\) is not met, namely, $k_{j+1} = k_j + 1$, and $\deg \beta[j]$ and $\text{ord}(\det \beta[j])$ are even, but $\xi_{\beta[j]} \neq 0$. Since $\deg \beta[j]$ is even, $[\beta[j]]$ has at least two diagonal entries, and thus, $[\beta[j]]$ and $[\beta]$ take the following forms:

\[
[\beta[j]] = \begin{pmatrix}
B' \\
0
\end{pmatrix}
\begin{pmatrix}
0 \\
2^{k_j} u_1
\end{pmatrix},
[\beta] = \begin{pmatrix}
[\beta[j]] \\
0
\end{pmatrix}
\begin{pmatrix}
0 \\
2^{k_j+1} u_2 \\
0
\end{pmatrix}.
\]

Here, $u_1$ is the last entry of $C_j$, $u_2$ is the first entry of $C_{j+1}$, and $B'$ is the diagonal submatrix of $[\beta[j]]$ obtained by removing its last diagonal $2^{k_j} u_1$ with $\deg B' \geq 1$.

If $\det B' = 2^k u_0$ with $u_0 \in \{1, 3, 5, 7\}$ and $k \in \mathbb{Z}_{\geq 0}$, then $\text{ord}(\det \beta[j]) = k + k_j$ is even. The condition $\xi_{\beta[j]} \neq 0$ means that $(-1)^{\deg \beta[j]}/2 u_0 u_1 \equiv 1$ or $5 \pmod{8}$, i.e. $c u_1 \equiv 1 \pmod{4}$ with $c = (-1)^{\deg \beta[j]/2} u_0 \pmod{8}$.

Let us describe a rule to replace these $u_1, u_2$ from $\beta$ into $u'_1, u'_2$ to get $\beta'$ such that $\xi_{\beta'[j]} = 0$ and

\[
[\beta] = \begin{pmatrix}
B' \\
0
\end{pmatrix}
\begin{pmatrix}
2^{k_j} u_1 \\
0
\end{pmatrix} \sim_{\mathbb{Z}_2} \begin{pmatrix}
B' \\
0
\end{pmatrix}
\begin{pmatrix}
2^{k_j} u'_1 \\
0
\end{pmatrix} = [\beta'].
\]

Note that the validity of Conditions \((\iota)\) and \((\ii)\) of Definition 1.5 are preserved under this type of operation. Since we have $\beta'[j] = \beta[j]$ for all $i < j$, applying it eventually produces a weak canonical form $\beta''$ such that $[\beta''] \sim_{\mathbb{Z}_2} [\beta]$.

**Lemma 2.3.** Let $c, u_1, u_2 \in \{1, 3, 5, 7\}$ be as above. Define $u'_1, u'_2 \in \{1, 3, 5, 7\}$ as follows (see Table 2):

- Suppose that $u_1 \not\equiv u_2 \pmod{4}$. Let $u'_1, u'_2 \in \{1, 3, 5, 7\}$ such that $u_i \not\equiv u'_i \pmod{4}$, and $(\frac{u_i}{2}) = \left(\frac{u'_i}{2}\right)$ for each $i = 1, 2$, and $u_1 + u_2 \equiv u'_1 + u'_2 \pmod{8}$;
Suppose that \( u_1 \equiv u_2 \pmod{4} \). Let \( u_i', u_j' \in \{1, 3, 5, 7\} \) such that \( u_i \not\equiv u_i' \pmod{4} \), and \( \left( \frac{u_i}{2} \right) \not\equiv \left( \frac{u_i'}{2} \right) \) for each \( i \in \{1, 2\} \), and \( u_1 + u_2 + 4 \equiv u_1' + u_2' \pmod{8} \).

We have \( cu_1' \equiv 3 \pmod{4} \), and \( (2^{k_j}u_1) \perp (2^{k_j+1}u_2) \sim_{\mathbb{Z}_2} (2^{k_j}u_1') \perp (2^{k_j+1}u_2') \).

Proof. As \( cu_1 \equiv 3 \pmod{4} \), \( cu_1' \equiv 1 \pmod{4} \). Regarding the second part of the statement, it is enough to show that \( (u_1) \perp (2u_2) \sim_{\mathbb{Z}_2} (u_1') \perp (2u_2') \). Let us borrow a few terms from [CS93] Section 7.5 of Chapter 15 for a simple proof. When \( u_1 \not\equiv u_2 \pmod{4} \), the genus symbols of \( (u_1) \perp (2u_2) \) and \( (u_1') \perp (2u_2') \) are the same up to the ‘oddity fusion’. When \( u_1 \equiv u_2 \pmod{4} \), the genus symbols of \( (u_1) \perp (2u_2) \) and \( (u_1') \perp (2u_2') \) are the same up to the ‘sign walk’.

| \( u_1 \not\equiv u_2 \pmod{4} \) | \( (u_1, u_2) \) | \( (u_1', u_2') \) | \( (u_1, u_2) \) | \( (u_1', u_2') \) |
|---|---|---|---|---|
| (1, 3) | (7, 3) | (5, 3) | (3, 5) |
| (1, 7) | (7, 1) | (5, 7) | (3, 1) |
| (3, 1) | (5, 7) | (7, 1) | (1, 7) |
| (3, 5) | (5, 3) | (7, 5) | (1, 3) |

| \( u_1 \equiv u_2 \pmod{4} \) | \( (u_1, u_2) \) | \( (u_1', u_2') \) | \( (u_1, u_2) \) | \( (u_1', u_2') \) |
|---|---|---|---|---|
| (1, 1) | (3, 3) | (5, 1) | (7, 3) |
| (1, 5) | (3, 7) | (5, 5) | (7, 7) |
| (3, 3) | (1, 1) | (7, 3) | (5, 1) |
| (3, 7) | (1, 5) | (7, 7) | (5, 5) |

Table 2. \( (u_1, u_2, u_1', u_2') \) satisfying the conditions in Lemma 2.3

The command \texttt{reduceWeakCanonical} follows the above procedure.

3. Table of intersection numbers of modular correspondences

In this section, we consider the formula of [GK93] for the arithmetic intersection number of three modular correspondences from a computational perspective. As mentioned in the Introduction, this is the original context in which the Gross-Keating invariants have been introduced for ternary quadratic forms over \( \mathbb{Z}_p \). Let us denote the set of non-degenerate half-integral matrices with entries in \( \mathbb{Z} \) by \( \mathcal{H}_n(\mathbb{Z})^{nd} \). We can regard \( Q \in \mathcal{H}_n(\mathbb{Z})^{nd} \) as an element of \( \mathcal{H}_n(\mathbb{Z}_p)^{nd} \) for any prime \( p \).

For \( m \in \mathbb{Z}_{\geq 1} \), let \( \phi_m(X, Y) \in \mathbb{Z}[X, Y] \) be the classical modular polynomial; see [GK93] and the references therein. Let \( m_1, m_2, m_3 \in \mathbb{Z}_{\geq 1} \). Gross and Keating showed that the cardinality of the quotient ring \( \mathbb{Z}[X, Y]/(\phi_{m_1}, \phi_{m_2}, \phi_{m_3}) \) is finite if and only if there is no positive definite binary quadratic form \( ax^2 + bxy + cy^2 \) with \( a, b, c \in \mathbb{Z} \) which represents the three integers \( m_1, m_2, m_3 \). Assume that \( m_1, m_2, m_3 \) satisfy this condition. Let \( S = \text{Spec} \mathbb{Z}[X, Y] \) and \( T_m \) be the divisor on \( S \) corresponding to \( \phi_m \). We define the arithmetic intersection number as follows:

\[
(T_{m_1} \cdot T_{m_2} \cdot T_{m_3})_S := \log \# \mathbb{Z}[X, Y]/(\phi_{m_1}, \phi_{m_2}, \phi_{m_3})
= \sum_p n(p) \log p,
\]

where

\[
\sum_p n(p) \log p.
\]
with \( n(p) = 0 \) for \( p > 4m_1m_2m_3 \). Furthermore, Gross and Keating found an explicit formula for \( n(p) \).

**Theorem 3.1.** [GK93, Proposition 3.22] Let \( p \) be a prime. We have

\[
n(p) = \frac{1}{2} \sum_{Q} \left( \prod_{l|\Delta, l \neq p} \beta_l(Q) \right) \cdot \alpha_p(Q),
\]

with \( \Delta = 4 \det Q \in \mathbb{Z} \). The sum is over all positive definite matrices \( Q \in \mathcal{H}_3(\mathbb{Z})^{\text{nd}} \) with diagonal \((m_1, m_2, m_3)\) which are isotropic over \( \mathbb{Q}_p \) for all \( l \neq p \). Such \( Q \) is anisotropic over \( \mathbb{Q}_p \) and \( p \) divides \( \Delta \). The quantities \( \alpha_p(Q) \) and \( \beta_p(Q) \) are given as follows:

Let \( H = (a_1, a_2, a_3; \varepsilon_1, \varepsilon_2, \varepsilon_3) \) be a naive EKG datum of \( Q \) at regarded as elements of \( \mathcal{H}_3(\mathbb{Z}_p)^{\text{nd}} \), as in [1,2].

When \( a_1 \equiv a_2 \pmod{2} \) and \( a_2 < a_3 \), we further define \( \varepsilon \) to be \( \varepsilon_2 \). If \( a_1 \equiv a_2 \pmod{2} \), then \( \alpha_p(Q) \) is equal to

\[
\sum_{i=0}^{a_1-1} (i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-1)/2} (a_1+1)(2a_1+a_2+a_3-4i)p^i + \frac{1}{2}(a_1+1)(a_3-a_2+1)p^{(a_1+a_2)/2}.
\]

If \( a_1 \not\equiv a_2 \pmod{2} \), then \( \alpha_p(Q) \) is equal to

\[
\sum_{i=0}^{a_1-1} (i+1)(a_1+a_2+a_3-3i)p^i + \sum_{i=a_1}^{(a_1+a_2-1)/2} (a_1+1)(2a_1+a_2+a_3-4i)p^i.
\]

If \( a_1 \equiv a_2 \pmod{2} \) and either \( \varepsilon = 1 \) or \( a_2 = a_3 \), then \( \beta_p(Q) \) is equal to

\[
\sum_{i=0}^{a_1-1} 2(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2} 2(a_1+1)p^i + (a_1+1)(a_3-a_2+1)p^{(a_1+a_2)/2}.
\]

If \( a_1 \equiv a_2 \pmod{2} \) and \( \varepsilon = -1 \), then \( \beta_p(Q) \) is equal to

\[
\sum_{i=0}^{a_1-1} 2(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2} 2(a_1+1)p^i + (a_1+1)p^{(a_1+a_2)/2}.
\]

If \( a_1 \not\equiv a_2 \pmod{2} \), then \( \beta_p(Q) \) is equal to

\[
\sum_{i=0}^{a_1-1} 2(i+1)p^i + \sum_{i=a_1}^{(a_1+a_2-2)/2} 2(a_1+1)p^i.
\]

We have produced tables of \( n(p) \) using this formula when \( 1 \leq m_1 \leq m_2 \leq m_3 \leq 30 \); see Tables 3 and 4. For this we take the following steps:

1. find triples \( m = (m_1, m_2, m_3) \) such that there is no positive definite binary integral quadratic form representing these integers;
(2) for such a triple $m$ and a prime $p \leq 4m_1m_2m_3$, find the list $L_2(m; p)$ of all positive definite matrices $Q \in H_3(\mathbb{Z})^{\text{nd}}$ with diagonal $(m_1, m_2, m_3)$, which are isotropic over $Q_l$ for all $l \neq p$;

(3) for $Q \in L_2(m; p)$, compute $\alpha_p(Q)$, and $\beta_l(Q)$ for primes $l | 4 \det Q$, $l \neq p$, and

$$n(p) = \frac{1}{2} \sum_{Q \in L_2(m; p)} \left( \prod_l \beta_l(Q) \right) \cdot \alpha_p(Q).$$

The last step is about computing a naive EGK datum of $Q$ over $\mathbb{Z}_p$, which is covered in Subsection 1.3. We focus on the first two steps here.

| $(m_1, m_2, m_3)$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 |
|------------------|---|---|---|---|----|----|----|----|----|----|----|----|----|----|
| (1,2,13)         | 450 | 108 | 36 | 156 | 28 | 72 | 18 | 10 | 34 | 8  | 22 | 8  |    |    |
| (1,2,21)         | 656 | 144 | 298 | 32 | 40 | 96 | 48 | 68 | 24 | 12 | 42 | 10 | 8  | 8  |
| (1,2,30)         | 738 | 324 | 108 | 486 | 88 | 216 | 108 | 144 | 84 | 32 | 104 | 19 | 58 | 16 |
| (1,3,11)         | 452 | 182 | 36 | 144 | 58 | 72 | 60 | 24 | 54 | 52 | 14 | 12 | 10 | 4  |
| (1,3,14)         | 604 | 144 | 290 | 24 | 104 | 96 | 60 | 32 | 60 | 84 | 22 | 16 | 28 | 20 |
| (1,3,26)         | 1060 | 252 | 508 | 336 | 132 | 12 | 132 | 56 | 81 | 136 | 32 | 28 | 68 | 28 |

Table 3. $n(p)$ for given $(m_1, m_2, m_3)$ and primes $2 \leq p \leq 43$
The first step of the above can be reformulated as follows:

**Proposition 3.2.** [G07, Proposition 3.5] Let \( m_1, m_2, m_3 \) be positive integers. The following are equivalent:

- There exists no positive definite integral binary quadratic form which represents \( m_1, m_2, \) and \( m_3. \)
- Every positive semi-definite half-integral symmetric matrix \( Q \) with diagonal \((m_1, m_2, m_3)\) is non-degenerate.

Whereas the first is difficult to use to check if \( m = (m_1, m_2, m_3) \) satisfies the given condition, the second condition is feasible for algorithmic treatment. The first condition is still useful to rule out a given \( m \) quickly by tabulating the first few coefficients of...
Note that we only need $L$ for a reasonably big finite set of positive-definite binary quadratic forms $ax^2 + bxy + cy^2$ of small $4ac - b^2$.

For a given $\underline{m} = (m_1, m_2, m_3), Q \in \mathcal{H}_3(\mathbb{Z})^{nd}$ takes the following form:

$$Q = \begin{pmatrix} m_1 & \frac{t_1}{2} & \frac{t_2}{2} \\ \frac{t_1}{2} & m_2 & \frac{t_3}{2} \\ \frac{t_2}{2} & \frac{t_3}{2} & m_3 \end{pmatrix}$$

with $t_i \in \mathbb{Z}$. For $Q$ to be positive semi-definite, $(t_1, t_2, t_3) \in \mathbb{Z}^3$ should satisfy the following inequalities for the principal minors:

$$4m_1m_2 - t_3^2 \geq 0, \quad t_1t_2t_3 - m_1t_1^2 - m_2t_2^2 - m_3t_3^2 + 4m_1m_2m_3 \geq 0.$$  \hfill (3.2)

When all such $(t_1, t_2, t_3)$, which forms a finite set, actually satisfies the strict inequalities in the above, then Theorem 3.1 applies for $(m_1, m_2, m_3)$. One may use checkGKtripleQ in our program for this procedure. There are 37 such triples $(m_1, m_2, m_3)$ with $1 \leq m_1 \leq m_2 \leq m_3 \leq 30$.

3.2. second step. Now we have a triple $(m_1, m_2, m_3)$ and the list $L_1(\underline{m})$ of positive definite matrix $Q \in \mathcal{H}_3(\mathbb{Z})^{nd}$ with diagonal $(m_1, m_2, m_3)$ satisfying (3.2). For each $Q \in L_1(\underline{m})$, let us find all primes $p$ such that $Q$ is anisotropic over $\mathbb{Q}_p$.

Lemma 3.3. \textsuperscript{[Cas78], Lemma 3.1.7]} Let $p$ be odd. Assume and that $Q$ is $\mathbb{Q}_p$-equivalent to $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$. If $\text{ord}_p(a_1) = \text{ord}_p(a_2) = \text{ord}_p(a_3)$, then $Q$ is isotropic.

To obtain a finite list of primes $p$ such that $Q$ is anisotropic over $\mathbb{Q}_p$, first find a diagonal matrix $Q'$ with diagonals $a_1, a_2, a_3 \in \mathbb{Z}$ such that $Q$ and $Q'$ are $\mathbb{Q}$-equivalent. Then $Q$ is isotropic over $\mathbb{Q}_p$ if $p \nmid 2a_1a_2a_3$ Lemma 3.3. Thus we only need to check whether $Q$ is anisotropic over $\mathbb{Q}_p$ for primes $p \mid 2a_1a_2a_3$, which is equivalent to the condition $(-a_1a_3, -a_2a_3) = -1$ involving the Hilbert symbol over $\mathbb{Q}_p$.

In this way, we obtain a subset $L_2(\underline{m})$ of $L_1(\underline{m})$ consisting of $Q \in L_1(\underline{m})$ such that $Q$ is anisotropic over $\mathbb{Q}_p$ for some unique prime $p$, and isotropic over $\mathbb{Q}_l$ for all $l \neq p$. For each prime $p$, let

$$L_2(\underline{m}; p) := \{ Q \in L_2(\underline{m}) : Q \text{ is anisotropic over } \mathbb{Q}_p \}.$$  

Note that we only need $L_2(\underline{m}; p)$ for $p \leq 4m_1m_2m_3$. See Table 5 for the sizes of $L_1(\underline{m}), L_2(\underline{m})$ and $L_2(\underline{m}; p)$ for some primes $p$. 

\begin{equation}
\theta_{a,b,c} = \sum_{(x,y) \in \mathbb{Z}^2} q^{ax^2 + bxy + cy^2}
\end{equation}
### 3.3. Reliability checks.

When \( m_1 = 1 \), we can calculate the resultant of \( \phi_{m_2}(X, X) \) and \( \phi_{m_3}(X, X) \) to obtain \( \prod_p p^{n(p)} \). It requires an explicit expression\(^2\) for \( \phi_m(X, Y) \); see, for example, [BLS12, BOS16] for a method to compute \( \phi_m \). We have checked the entries with \( m_1 = 1 \) in Tables 3 and 4 by calculating the resultants of these polynomials, and obtained the agreement.

**Example 3.4.** There are values of \( n(p) \) for \((m_1, m_2, m_3) = (1, 3, 10)\) in [GK93], which is computed by Elkies using the resultant of the polynomials \( \phi_3(X, X) \) and \( \phi_{10}(X, X) \); this seems to be the unique example that had appeared in the literature. We can calculate \( n(p) \) for \((m_1, m_2, m_3) = (1, 3, 10) \) and \( p = 2 \) in our program as follows:

\(^2\)The data for \( \phi_m \) is available at [https://math.mit.edu/~drew/ClassicalModPolys.html](https://math.mit.edu/~drew/ClassicalModPolys.html).
\begin{align*}
\text{In[23]}:= & \quad \text{computeGKint}\{1,3,10\}, 2 \\
\text{Out[23]}=& \quad 452
\end{align*}
which matches Elkies’ computation.

\section*{Acknowledgements}

The author thanks Sungmum Cho and Hidenori Katsurada for kindly explaining their results with patience. He thanks Cris Poor, Jerry Shurman and David Yuen for allowing their code for Jordan decomposition to be included in \textit{computeGK} with modifications. He also thanks Richard Borcherds for mentioning Katsurada’s work in a conversation many years ago.

\section*{References}

\begin{thebibliography}{99}
\bibitem[BLS12]{BLS12} R. Bröker, K. Lauter, and A. V. Sutherland, \textit{Modular polynomials via isogeny volcanoes}, Math. Comp. \textbf{81} (2012), no. 278, 1201–1231.
\bibitem[BOS16]{BOS16} J. H. Bruinier, K. Ono, and A. V. Sutherland, \textit{Class polynomials for nonholomorphic modular functions}, J. Number Theory \textbf{161} (2016), 204–229.
\bibitem[Cas78]{Cas78} J. W. S. Cassels, \textit{Rational quadratic forms}, Academic Press, Inc., London-New York, 1978.
\bibitem[CIKY17]{CIKY17} S. Cho, T. Ikeda, H. Katsurada, and T. Yamauchi, \textit{Remarks on the Extended Gross-Keating data and the Siegel series of a quadratic form}, ArXiv e-prints (2017).
\bibitem[CS93]{CS93} J. H. Conway and N. J. A. Sloane, \textit{Sphere packings, lattices and groups}, second ed., Springer-Verlag, New York, 1993.
\bibitem[CY18]{CY18} S. Cho and T. Yamauchi, \textit{An inductive formula of the Gross-Keating invariant of a quadratic form}, preprint (2018).
\bibitem[Gö7]{Gö7} U. Görtz, \textit{Arithmetic intersection numbers}, Astérisque (2007), no. 312, 15–24.
\bibitem[GK93]{GK93} B. H. Gross and K. Keating, \textit{On the intersection of modular correspondences}, Invent. Math. \textbf{112} (1993), no. 2, 225–245.
\bibitem[IK15]{IK15} T. Ikeda and H. Katsurada, \textit{On the Gross-Keating invariant of a quadratic form over a non-archimedean local field}, ArXiv e-prints (2015).
\bibitem[IK16]{IK16} \textit{An explicit formula for the Siegel series of a quadratic form over a non-archimedean local field}, ArXiv e-prints (2016).
\bibitem[Kat99]{Kat99} H. Katsurada, \textit{An explicit formula for Siegel series}, Amer. J. Math. \textbf{121} (1999), no. 2, 415–452.
\bibitem[Kin03]{Kin03} O. D. King, \textit{A mass formula for unimodular lattices with no roots}, Math. Comp. \textbf{72} (2003), no. 242, 839–863.
\bibitem[KPSY18]{KPSY18} O. D. King, C. Poor, J. Shurman, and D. S. Yuen, \textit{Using Katsurada’s determination of the Eisenstein series to compute Siegel eigenforms}, Math. Comp. \textbf{87} (2018), no. 310, 879–892.
\bibitem[Kud97]{Kud97} S. S. Kudla, \textit{Central derivatives of Eisenstein series and height pairings}, Ann. of Math. (2) \textbf{146} (1997), no. 3, 545–646.
\bibitem[Wat60]{Wat60} G. L. Watson, \textit{Integral quadratic forms}, Cambridge University Press, New York, 1960.
\bibitem[Wed07]{Wed07} T. Wedhorn, \textit{Calculation of representation densities}, Astérisque (2007), no. 312, 179–190.
\end{thebibliography}

School of Mathematics, Korea Institute for Advanced Study, Seoul 130-722, Korea

E-mail address: chlee@kias.re.kr