An algorithm for the explicit evaluation of GL(n) Kloosterman sums

Version: 21st September 2005

Kevin A. Broughan

Department of Mathematics, University of Waikato,
Hamilton, New Zealand
E-mail: kab@waikato.ac.nz

An algorithm for the explicit evaluation of Kloosterman sums for $GL(n,\mathbb{R})$ for $n \geq 2$ and an implementation in the Mathematica package GL(n)pack are described.

Key Words: Kloosterman sum, Plücker coordinates, Plücker relations, symbolic-numeric algorithm.

MSC2000: 11L03, 11L05.

1. INTRODUCTION

Classical Kloosterman sums arise naturally as part of the Fourier coefficients of Poincaré series for GL(2) and have numerous applications in number theory. See for example [4]. The same is true of their generalization to series for GL(n) [6, 7, 2, 3]. In the main these sums are a theoretical tool. Sums have been presented in dimensions 3 and 4 as rather complicated abstract sums with symbolic coefficients satisfying constraints which have to be determined. It is the object of this paper to describe an algorithm, as implemented in the Mathematica package GL(n)pack [1], which will give an explicit exponential sum for GL(n) when a valid sum exists and indicate when no valid sum exists.

Computing such as sum involves choosing a complete set of matrix representatives in a double coset space, so the algorithm, as expected, has exponential complexity in one of the natural parameters. Finding a sub-exponential algorithm is an unsolved problem, but at least this work provides a start to the algorithmic development of these generalized sums.

In section 1 the definition and preliminary results, mostly from [7], are set out. Then in section 2 the central object on which the algorithm works, the Plücker relations, are discussed. Since these have many uses outside of the study of GL(n), the functions provided in the package for their construction may be of some independent use. The algorithm is described in section 3 and some comments made about its symbolic-numeric nature. The GL(n)pack implementation is discussed and, finally, some examples are given.

2. DEFINITIONS

Let $U = U_n(\mathbb{R})$ be the subgroup of upper triangular unipotent matrices (i.e. with 1's down the leading diagonal) , θ_1 a list of $n-1$ integers representing a character of $U_n(\mathbb{R})$ which is trivial on $\Gamma = SL(n,\mathbb{Z})$,$\Gamma_\infty = U \cap \Gamma$, θ_2 a list of $n-1$ integers representing another character of $U_n(\mathbb{R})$, c a list of $n-1$ non-zero integers specifying the diagonal of a matrix. The 1st diagonal element of the matrix is $det(w)/c_{n-1}$, the second c_{n-1}/c_{n-2} and so on down to the last c_1. This is the so-called "Friedberg form".

The function implementing the algorithm described here computes the generalized Kloosterman sum for $SL(n,\mathbb{Z})$ for $n \geq 2$. When $n = 2$ this coincides with the classical Kloosterman sum. More generally the sum is

$$S(\theta_1, \theta_2, c, w) := \sum_{\gamma = b_1 c w b_2} \theta_1(b_1)\theta_2(b_2)$$

where

$$\gamma \in \Gamma_\infty \backslash \Gamma \cap G_w / \Gamma_w$$

and $\Gamma_w = {}^t w.{}^t\Gamma_\infty.w \cap \Gamma_\infty$ and G_w is the Bruhat cell associated to the permutation matrix w. In other words, w is an $n \times n$ matrix which is zero except for a single 1 in each row and column, representing an explicit element of the Weyl subroup W_n of $GL(n,\mathbb{R})$.

Let L_i be the set of i element ordered subsets of $\{1, 2, \cdots, n\}$ with L_i ordered lexically. Given $\lambda \in L_i$ and $\gamma \in GL(n)$ denote by v_λ the $i \times i$ minor of γ formed from the bottom i rows and from the columns indexed by the elements of λ in increasing order. Let $V \subset \mathbb{R}^{2^n - 2}$ be an algebraic set of values of minor vectors $v = (v_\lambda)$ described in detail in [6, Page 3-07] or [8, Chapter XI].

3. PRELIMINARY RESULTS

Lemma 3.1. *[6, Equation (2) page 3-03] The Kloosterman sum $S(\theta_1, \theta_2, c, w)$ is well defined only when for all $(u \in {}^t w.U.w) \cap U$ we have $\theta_1(c.w.u.{}^t w c^{-1}) = \theta_2(u)$.*

Lemma 3.2. *[8, Proposition 10.3.6] Every $\gamma \in GL(n,\mathbb{R})$ has a Bruhat decomposition $\gamma = u_1 c w u_2$ with $u_1, u_2 \in U_n(\mathbb{R})$ and c in Friedberg form.*

Lemma 3.3. *[6, Proposition 1] Let γ in G_w have a Bruhat decomposition $\gamma = b_1 c w b_2$ with c a diagonal matrix in Friedberg form. Then, for $1 \leq i \leq n-1$, $c_i = M_{\lambda_i}(\gamma)$ with $\lambda_i = \{\omega(n), \omega(n-1), \cdots, \omega(n-i+1)$, ω being the permutation with matrix w, and $M_\lambda = 0$ whenever $\lambda < \lambda_i$, the ordering being lexical.*

Lemma 3.4. *[7, Proposition 1.4] Let $\gamma \in \Gamma$ have Bruhat decomposition $\gamma = b_1 c w b_2$ with $b_1, b_2 \in U_n(\mathbb{R})$ and c a diagonal matrix. Then c is uniquely determined.*

Lemma 3.5. *[6, Theorem 2] Let $M(\gamma) = (M_\lambda(\gamma) | \lambda \in L_1 \cup \cdots L_{n-1})$. Then the mapping $\gamma \to M(\gamma)$ from $GL(n,\mathbb{R})$ to V is onto and induces a bijection from $\Gamma_\infty \backslash \Gamma$ to*

$$V' = \{v \in V | \textit{for all } \lambda, v_\lambda \in \mathbb{Z}, GCD(v_\lambda | \lambda \in L_k) = 1, \textit{for all } 1 \leq k \leq n-1\}.$$

Lemma 3.6. *[6, Theorem 2] If $\gamma, \gamma' \in \Gamma \cap G_w$, then $\Gamma_\infty \gamma \Gamma_w = \Gamma_\infty \gamma' \Gamma_w$ if and only if $M_{\lambda_i}(\gamma) = M_{\lambda_i}(\gamma')$ for all i with $1 \leq i \leq n-1$ and $M_\lambda(\gamma) \equiv M_\lambda(\gamma') \bmod M_{\lambda_i}(\gamma)$ for all $\lambda \in L_i$.*

Here is a description of the strategy, based on these lemmas, employed to compute the sums: a set of integer vectors which satisfy the necessary constraints implied by these results is formed. These are potential Plücker coordinates of elements of $SL(n,\mathbb{Z})$. This set is reduced by retaining only those vectors which satisfy all known Plücker relations for that dimension. Then each remaining vector is inverted, i.e. a matrix γ is found having those Plücker coordinates. Even though a proof is not at hand, it is the writers belief that the existing set of Plücker relations, for general n, is sufficiently large to ensure that each set of coordinates arises from an integer matrix. In the event that the set of relations is not complete then the inversion process will fail and the vector will be discarded. Following inversion a Bruhat decomposition is applied to derive the unipotent vectors b_1 and b_2 which solve the matrix equation $\gamma = b_1.w.c.b_2$. These vectors are then used to form the sum which is returned.

4. PLÜCKER COORDINATES AND RELATIONS

The GL(n)pack function **PluckerRelations** computes recursively a set of quadratic forms in the bottom row based minor determinants of any $n \times n$ matrix in $GL(n, \mathbb{R})$. These forms have coefficients ± 1. They must vanish if the values assigned to symbols representing the minor determinants come from any square matrix. The number of Plücker relations grows rapidly with n, because each $j \times j$ sub-matrix, with elements chosen from the bottom j rows and any j columns, also gives rise to a set of relationships of the given type. In dimension 2 there are no relationships and in 3 just one, the Cramer's rule relationship $v_1v_{23} - v_2v_{13} + v_3v_{12} = 0$, denoted $P_{3,1}$. (Here the Friedberg notation v_λ, where λ is an ordered subset of $\{1, 2, \cdots, n\}$, is used to represent the minor determinant based on the bottom $|\lambda|$ rows and the columns indexed by the elements of λ). In this example ten relationships for dimension $n = 4$ are derived and how this is generalized to general n indicated.

1. The simplest relationship is obtained by expanding the matrix using the bottom row based minors of size $n - 1$ along the bottom row. By Cramer's rule the form

$$(-1)^{1+1}v_1v_{234} + (-1)^{1+2}v_2v_{134} + (-1)^{1+3}v_3v_{124} + (-1)^{1+4}v_4v_{123}$$

necessarily vanishes, i.e.

$$v_1v_{234} - v_2v_{134} + v_3v_{124} - v_4v_{123} = 0,$$

$(P_{4,1})$.

2. Now let the rows of a fixed but arbitrary 4×4 matrix be represented by the vectors a_1, a_2, a_3, a_4, indexed from the bottom row up. Then because for all vectors v, $v \wedge v = 0$:

$$0 = (a_2 \wedge a_1) \wedge (a_2 \wedge a_1) = \lambda\, e_1 \wedge e_2 \wedge e_3 \wedge e_4,$$

where the e_i are the standard unit vectors and λ is a real constant with value $v_{12}v_{34} - v_{24}v_{13} + v_{14}v_{23}$, which is therefore 0. This is $P_{4,2}$.

3. The relationship

$$v_{24}v_{123} + v_{12}v_{234} - v_{23}v_{124} = 0$$

is now derived. First expand the wedge product of the bottom two rows:

$$\begin{aligned} a_2 \wedge a_1 &= v_{12}e_1 \wedge e_2 + v_{13}e_1 \wedge e_3 + v_{14}e_1 \wedge e_4 \\ &\quad + v_{23}e_2 \wedge e_3 + v_{24}e_2 \wedge e_4 + v_{34}e_3 \wedge e_4. \end{aligned}$$

Then

$$\begin{aligned} a_2 \wedge a_1 &= e_2 \wedge (-v_{12}e_1 + v_{23}e_3 + v_{24}e_4) \\ &\quad + v_{13}e_1 \wedge e_3 + v_{14}e_1 \wedge e_4 + v_{34}e_3 \wedge e_4 \\ &= e_2 \wedge \omega + \eta, \end{aligned}$$

say, where ω is a 1-form and η a 2-form with e_2 not appearing. Then

$$a_3 \wedge a_2 \wedge a_1 = v_{123} e_1 \wedge e_2 \wedge e_3 + v_{234} e_2 \wedge e_3 \wedge e_4 + v_{124} e_1 \wedge e_2 \wedge e_4$$

so

$$\begin{aligned} a_3 \wedge a_2 \wedge a_1 \wedge \omega &= (v_{24} v_{123} + v_{12} v_{234} - v_{23} v_{124}) e_1 \wedge e_2 \wedge e_3 \wedge e_4 + 0 \\ &= \lambda\, e_1 \wedge e_2 \wedge e_3 \wedge e_4 \end{aligned}$$

say.

Since each term of η has two of $\{e_1, e_3, e_4\}$ and each term of ω one of this set we can write

$$\eta \wedge \omega = (v_{12} v_{34} - v_{24} v_{13} + v_{14} v_{23}) e_1 \wedge e_3 \wedge e_4 = 0$$

by the relation $P_{4,2}$ derived in 2. above.

But then

$$\begin{aligned} a_3 \wedge a_2 \wedge a_1 \wedge \omega &= a_3 \wedge (a_2 \wedge a_1) \wedge \omega \\ &= a_3 \wedge (e_2 \wedge \omega + \eta) \wedge \omega \\ &= a_3 \wedge (\eta \wedge \omega) = 0 \end{aligned}$$

so therefore $\lambda = 0$ and we have derived the relation $P_{4,3}$:

$$v_{24} v_{123} + v_{12} v_{234} - v_{23} v_{124} = 0.$$

Three similar relationships $P_{4,4}, P_{4,5}, P_{4,6}$ are derived by factoring out in turn each of the unit vectors e_1, e_3 and e_4.

4. The four remaining relations are obtained by applying the dimension 3 relationship to each of the four subsets of $\{1, 2, 3, 4\}$ of column numbers of size 3.

5. The approach described in 2.-4. above works also for $n = 5$. In summary if we let $a_1 \wedge a_2 = e_1 \wedge \omega + \eta$ then $a_1 \wedge a_2 \wedge \omega = 0$ because $\eta \wedge \omega = 0$. This latter equation follows from relations such as $v_{14} v_{23} + v_{13} v_{24} + v_{12} v_{34} = 0$, a subset relation for $n = 5$ following from the $n = 4$ case.

6. For general n most relations are derived simply by expanding the left hand side of $(a_1 \wedge \cdots \wedge a_i) \wedge (a_1 \wedge \cdots a_j) = 0$ for $1 \le i \le j$ with $i + j \le n$ and $i < j$ if $i = 1$, and deriving subset relations for each m with $2 \le m < n$.

7. In addition to the above, for each subset $S \subset \{1, 2, \cdots, n\}$ of size $n - 3$ the so called "top-level" three term relation is derived. Each of these is similar to the following example given for dimension 6 where $S = \{1, 2, 3\}$:

$$v_{1234}\, v_{12356} - v_{1235}\, v_{12346} + v_{1236}\, v_{12345} = 0.$$

8. As of the date of this paper the GL(n)pack function PluckerRelations derives the following sets of relations: 0 in dimension 2, 1 in 3, 10 in 4, 57 in 5, 255 in 6 and 969 in 7.

Relation for $\mathbf{n = 3}$:

$$P_{3,1} : \; v_1 v_{23} - v_2 v_{23} + v_3 v_{12} = 0$$

Relations for $\mathbf{n=4}$:

$$P_{4,1}: \quad v_4v_{123} - v_3v_{124} + v_2v_{134} - v_1v_{234} = 0,$$

$$\begin{aligned}
P_{4,2}: &\quad v_{14}v_{23} - v_{13}v_{24} + v_{12}v_{34} = 0,\\
P_{4,3}: &\quad v_{24}v_{123} - v_{23}v_{124} + v_{12}v_{234} = 0,\\
P_{4,4}: &\quad v_{34}v_{123} - v_{23}v_{134} + v_{13}v_{234} = 0,\\
P_{4,5}: &\quad v_{34}v_{124} - v_{24}v_{134} + v_{14}v_{234} = 0,\\
P_{4,6}: &\quad v_{14}v_{123} - v_{13}v_{124} + v_{12}v_{134} = 0.
\end{aligned}$$

$$\begin{aligned}
P_{4,7}: &\quad v_3v_{12} - v_2v_{13} + v_1v_{23} = 0,\\
P_{4,8}: &\quad v_4v_{12} - v_2v_{14} + v_1v_{24} = 0,\\
P_{4,9}: &\quad v_4v_{13} - v_3v_{14} + v_1v_{34} = 0,\\
P_{4,10}: &\quad v_4v_{23} - v_3v_{24} + v_2v_{24} = 0.
\end{aligned}$$

Relations for $\mathbf{n=5}$:

$$\begin{aligned}
P_{5,1}: &\quad v_{45}\,v_{123} - v_{35}\,v_{124} + v_{34}\,v_{125} + v_{25}\,v_{134} - v_{24}\,v_{135}\\
&+ v_{23}\,v_{145} - v_{15}\,v_{234} + v_{14}\,v_{235} - v_{13}\,v_{245} + v_{12}\,v_{345} = 0,\\
P_{5,2}: &\quad v_5\,v_{1234} - v_4\,v_{1235} + v_3\,v_{1245} - v_2\,v_{1345} + v_1\,v_{2345} = 0,\\
P_{5,3}: &\quad v_{345}\,v_{1245} - v_{245}\,v_{1345} + v_{145}\,v_{2345},\\
P_{5,4}: &\quad v_{345}\,v_{1235} - v_{235}\,v_{1345} + v_{135}\,v_{2345},\\
P_{5,5}: &\quad v_{345}\,v_{1234} - v_{234}\,v_{1,345} + v_{1,34}\,v_{2345},\\
P_{5,6}: &\quad v_{245}\,v_{123,5} - v_{235}\,v_{1245} + v_{12,5}\,v_{2345},\\
P_{5,7}: &\quad v_{2,45}\,v_{1234} - v_{234}\,v_{1245} + v_{124}\,v_{2345},\\
P_{5,8}: &\quad v_{235}\,v_{1234} - v_{234}\,v_{1235} + v_{123}\,v_{2345},\\
P_{5,9}: &\quad v_{145}\,v_{1235} - v_{135}\,v_{1245} + v_{125}\,v_{1345},\\
P_{5,10}: &\quad v_{145}\,v_{1234} - v_{134}\,v_{1245} + v_{124}\,v_{1345},\\
P_{5,11}: &\quad v_{135}\,v_{1234} - v_{134}\,v_{1235} + v_{123}\,v_{1345},\\
P_{5,12}: &\quad v_{125}\,v_{1234} - v_{124}\,v_{1235} + v_{123}\,v_{1245},\\
P_{5,13}: &\quad v_{15}\,v_{1234} - v_{14}\,v_{1235} + v_{13}\,v_{1245} - v_{12}\,v_{1345} = 0,\\
P_{5,14}: &\quad v_{25}\,v_{1234} - v_{24}\,v_{1235} + v_{23}\,v_{1245} - v_{12}\,v_{2345} = 0,\\
P_{5,15}: &\quad v_{35}\,v_{1234} - v_{34}\,v_{1235} + v_{23}\,v_{1345} - v_{13}\,v_{2345} = 0,\\
P_{5,16}: &\quad v_{45}\,v_{1234} - v_{34}\,v_{1245} + v_{24}\,v_{1345} - v_{14}\,v_{2345} = 0,\\
P_{5,17}: &\quad v_{45}\,v_{1235} - v_{35}\,v_{1245} + v_{25}\,v_{1345} - v_{15}\,v_{2345} = 0,\\
P_{5,18}: &\quad v_4\,v_{123} - v_3\,v_{124} + v_2\,v_{134} - v_1\,v_{234} = 0,\\
P_{5,19}: &\quad v_5\,v_{134} - v_4\,v_{135} + v_3\,v_{145} - v_1\,v_{345} = 0,\\
P_{5,20}: &\quad v_5\,v_{234} - v_4\,v_{235} + v_3\,v_{245} - v_2\,v_{345} = 0,\\
P_{5,21}: &\quad v_5\,v_{123} - v_3\,v_{125} + v_2\,v_{135} - v_1\,v_{235} = 0,\\
P_{5,22}: &\quad v_5\,v_{124} - v_4\,v_{125} + v_2\,v_{145} - v_1\,v_{245} = 0,\\
P_{5,23}: &\quad v_{14}\,v_{123} - v_{13}\,v_{124} + v_{12}\,v_{134} = 0,\\
P_{5,24}: &\quad v_{15}\,v_{123} - v_{13}\,v_{125} + v_{12}\,v_{135} = 0,\\
P_{5,25}: &\quad v_{15}\,v_{124} - v_{14}\,v_{125} + v_{12}\,v_{145} = 0,\\
P_{5,26}: &\quad v_{15}\,v_{134} - v_{14}\,v_{135} + v_{13}\,v_{145} = 0,\\
P_{5,27}: &\quad v_{24}\,v_{123} - v_{23}\,v_{124} + v_{12}\,v_{234} = 0,\\
P_{5,28}: &\quad v_{34}\,v_{123} - v_{23}\,v_{134} + v_{13}\,v_{234} = 0,\\
P_{5,29}: &\quad v_{34}\,v_{124} - v_{24}\,v_{134} + v_{14}\,v_{234} = 0,\\
P_{5,30}: &\quad v_{25}\,v_{123} - v_{23}\,v_{125} + v_{12}\,v_{235} = 0,\\
P_{5,31}: &\quad v_{35}\,v_{123} - v_{23}\,v_{135} + v_{13}\,v_{235} = 0,\\
P_{5,32}: &\quad v_{35}\,v_{125} - v_{25}\,v_{135} + v_{15}\,v_{235} = 0.
\end{aligned}$$

$$
\begin{aligned}
P_{5,33}: &\quad v_{25}\,v_{124}-v_{24}\,v_{125}+v_{12}\,v_{245}=0,\\
P_{5,34}: &\quad v_{45}\,v_{124}-v_{24}\,v_{145}+v_{14}\,v_{245}=0,\\
P_{5,35}: &\quad v_{45}\,v_{125}-v_{25}\,v_{145}+v_{15}\,v_{245}=0,\\
P_{5,36}: &\quad v_{25}\,v_{234}-v_{24}\,v_{235}+v_{23}\,v_{245}=0,\\
P_{5,37}: &\quad v_{35}\,v_{134}-v_{34}\,v_{135}+v_{13}\,v_{345}=0,\\
P_{5,38}: &\quad v_{45}\,v_{134}-v_{34}\,v_{145}+v_{14}\,v_{345}=0,\\
P_{5,39}: &\quad v_{45}\,v_{135}-v_{35}\,v_{145}+v_{15}\,v_{345}=0,\\
P_{5,40}: &\quad v_{35}\,v_{234}-v_{34}\,v_{235}+v_{23}\,v_{345}=0,\\
P_{5,41}: &\quad v_{45}\,v_{234}-v_{34}\,v_{245}+v_{24}\,v_{345}=0,\\
P_{5,42}: &\quad v_{45}\,v_{235}-v_{35}\,v_{245}+v_{25}\,v_{345}=0,\\
P_{5,43}: &\quad v_{15}\,v_{24}-v_{14}\,v_{25}+v_{12}\,v_{45}=0,\\
P_{5,44}: &\quad v_{15}\,v_{34}-v_{14}\,v_{35}+v_{13}\,v_{45}=0,
\end{aligned}
$$

$$
\begin{aligned}
P_{5,45}: &\quad v_{25}\,v_{34}-v_{24}\,v_{35}+v_{23}\,v_{45}=0,\\
P_{5,46}: &\quad v_{14}\,v_{23}-v_{13}\,v_{24}+v_{12}\,v_{34}=0,\\
P_{5,47}: &\quad v_{15}\,v_{23}-v_{13}\,v_{25}+v_{12}\,v_{35}=0,\\
P_{5,48}: &\quad v_{5}\,v_{13}-v_{3}\,v_{15}+v_{1}\,v_{35}=0,\\
P_{5,49}: &\quad v_{5}\,v_{23}-v_{3}\,v_{25}+v_{2}\,v_{35}=0,\\
P_{5,50}: &\quad v_{3}v_{12}-v_{2}\,v_{13}+v_{1}\,v_{23}=0,\\
P_{5,51}: &\quad v_{4}\,v_{12}-v_{2}\,v_{14}+v_{1}\,v_{24}=0,\\
P_{5,52}: &\quad v_{5}\,v_{12}-v_{2}\,v_{15}+v_{1}\,v_{25}=0,\\
P_{5,53}: &\quad v_{4}\,v_{13}-v_{3}\,v_{14}+v_{1}\,v_{34}=0,\\
P_{5,54}: &\quad v_{4}\,v_{23}-v_{3}\,v_{24}+v_{2}\,v_{34}=0,\\
P_{5,55}: &\quad v_{5}\,v_{14}-v_{4}\,v_{15}+v_{1}\,v_{45}=0,\\
P_{5,56}: &\quad v_{5}\,v_{24}-v_{4}\,v_{25}+v_{2}\,v_{45}=0,\\
P_{5,57}: &\quad v_{5}\,v_{34}-v_{4}\,v_{35}+v_{3}\,v_{45}=0.
\end{aligned}
$$

Some remarks: The GL(n)pack function PluckerRelations computes all the known quadratic relationships between the Plücker coordinates, namely the set of bottom rows based minors of a generic square $n \times n$ matrix. In case $n = 2$ there are none and for $n = 3$ one. For $n > 3$ the number grows dramatically. No claim is made that this function returns, for any given n, a complete set of independent relationships. In dimensions 3,4 and 5 the writer believes the set is complete in the strong sense that there are no other general quadratic relations between bottom row based minors. The relations computed for dimension 3 through 7 have been validated by evaluating the relation on a symbolic matrix and seeing that the left hand side of each one reduces to zero. They include the relations described in [5].

5. ALGORITHM DESCRIPTION

These are the steps employed in the function KloostermanSum included in GL(n)pack . Here suppose the arguments are θ_1, θ_2, c and w where the first two arguments are characters on $U_n(\mathbb{R})$, c is a list of $n-1$ non-zero integers and w an $n \times n$ permutation matrix.

1. First check the number of arguments, the data types of the arguments and get the dimension n.

2. Get the so called c_i constraints, $v_{\lambda_i} \to c_i$, and call these $\mathcal{C}_{\mathcal{M}}$. See Lemma 3.2.

3. Get the lexical constraints $v_\lambda \to 0$ for all $\lambda < \lambda_i$ and call these $\mathcal{C}_{\mathcal{L}}$. See Lemma 3.2.

4. Form the Plücker relations for dimension n and call these $\mathcal{P}$.

5. Reduce the Plücker relations $\mathcal{P}$ by applying the constraints $\mathcal{C}_{\mathcal{M}}$ and $\mathcal{C}_{\mathcal{L}}$ to form a new (smaller) set of relations $\mathcal{P}'$ which are functions of the c_i as well as the v_λ.

6. If this reduced set of relations results in the necessary vanishing of minors additional to those found in 3 reduce the set of relations further by substituting 0 for each such minor and call the resulting relations $\mathcal{P}''$.

7. Using $\mathcal{P}''$ and the compatibility relation between characters $\theta_1(c.w.u.w^{-1}.c^{-1}) = \theta_2(u)$ for all $u \in {}^t w {}^t U w \cap U$ where $U = U_n(\mathbb{R})$ is the upper triangular unipotent matrix group. See [Friedberg,

1985-86, eqn. (2)]. Then check (a) that the characters are compatible and (b) derive any divisibility relations between the c_i.

These divisibilities are derived as follows: if all of the minors $\mathcal{L}_i$ at a given level i vanish except for $v_{\lambda_i} = c_i$ then the relation $\mathrm{gcd}(\mathrm{v}_\lambda : \lambda \in \mathcal{L}_\mathrm{i}) = 1$ (Lemma 3.3) implies $c_i \mid 1$ so return $\{c_i, 1\}$. Then, for each distinct pair of indices i, j extract all of the reduced Plücker relations $\mathcal{P}''$ which contain four terms

$$\pm c_i v_1 \pm c_j v_2 = 0.$$

If any subset S of the $v_2's$ satisfies $\mathrm{gcd}(\mathrm{c_j}, \mathrm{v_2} : \mathrm{v_2} \in \mathrm{S}) = 1$ then necessarily $c_i \mid c_j$ so return $\{c_i, c_j\}$.

8. For each i with $1 \le i \le n-1$, form the set $\mathcal{M}_i$ of all vectors of $\binom{n}{i}$ integers m_λ with $0 \le m_\lambda < c_i$ with the m_λ being the minor representatives with $|\lambda| = i$, and such that the constraints $\mathcal{C}_\mathcal{M}$ and $\mathcal{C}_\mathcal{L}$ are satisfied and the so-called GCD constraints $\mathrm{gcd}(\mathrm{m}_\lambda : \lambda \in \mathcal{L}_\mathrm{i}) = 1$ are also satisfied.

9. Form the product $\mathcal{V} = \prod_{i=1}^{n-1} \mathcal{M}_i$.

10. For each vector $v \in \mathcal{V}$, test to see whether it can be identified with the vector of minors of an element of SL(n,$\mathbb{Z}$) as follows: If each relation in $\mathcal{P}''$ vanishes when the corresponding integer values from v are substituted, retain v, otherwise discard it. Call the reduced set of vectors $\mathcal{V}'$.

11. For each $v \in \mathcal{V}'$, invert using PluckerInvert (see below) to find a matrix $a_v \in SL(n, \mathbb{Z})$, which has v as its Plücker coordinates, and which satisfies

$$a_v = x_v.c.w.y_v$$

for unipotent matrices x_v, y_v in $U_n(\mathbb{Q})$. These are found by applying the GL(n)pack function BruhatForm to a_v.

A note regarding the technique employed to invert the Plücker coordinates: from a vector $v \in \mathcal{V}'$, a matrix $a_v = (a_{i,j}) \in SL(n, \mathbb{Z})$, having v as its Plücker coordinates, is derived row by row. First the top row is computed using the extended GCD algorithm to solve the cofactor expansion equation

$$1 = \sum_{j=1}^{n} (-1)^{1+j} a_{1,j} v^j,$$

where v^j is the appropriate minor, an element of v. Then for each row i with $2 \le i \le n-1$, solve the system of integer equations

$$v_\lambda = \sum_{j \in \lambda} (-1)^{i+j} a_{i,j} v^j, \lambda \in \mathcal{L}_i.$$

For row n set $a_{n,j} = v_{\{j\}}$ where $\lambda = \{j\}$.

It is clear that when this stepwise solution process returns a matrix a, its Plücker coordinates must be v. At row i, $\binom{n}{n-i+1}$ integer equations in n integer unknowns are solved using the built in Mathematica function Reduce. If Reduce gives no solution for any row then vector v is removed from $\mathcal{V}'$. Hence is is essential that Reduce gives a correct integer solution when one exists and no solution when and only when no solution exists.

The function Reduce was validated in the following manner: 100 random integer matrixes A of dimension 40×25 and random vectors x of dimension 40 were generated. In each case the value of b was computed and then the matrix equation $x.A = b$ solved over the integers, using Reduce, successfully. When b was chosen at random in each case with 100 random matrices A the system failed to solve. Because of this it was decided that a hand crafted function, and presumably slower because it was written in top-level Mathematica code, using the Hermite Normal Form to solve the integer system or determine no integer solution existed, was unnecessary.

12. Finally form and simplify the sum $\sum_{v\in\mathcal{V}'}\theta_1(x_v)\theta_2(y_v)$.

The proof that this approach the sum works is a direct consequence of the lemmas. 3.2, 3.3 and 3.4. Since w and c are fixed, only those integer vectors, being potential Plücker coordinates of matrices in SL(n,Z), are considered in which satisfy the constraints $v_{\lambda_i}(\gamma) = c_i$, $v\lambda(\gamma) = 0$ for $\lambda < \lambda_i$ and $GCD(v_\lambda(\gamma)|\lambda \in L_k) = 1$. A representative is chosen for consideration in each equivalence class modulo c_i. The Plücker relations are used (when complete) to cull this set of vectors to ensure each set comes from a matrix in SL(n,Z). Since the constraints are satisfied, the matrix will automatically have the form $b_1.c.w.b_2$. When not complete the inversion process fails, leading again to removal of the vector.

Theorem 5.1. *The algorithm gives the correct value for a valid Kloosterman sum.*

Proof. 1. Let $\gamma \in \Gamma \cap G_w$ have $M_{\lambda_i}(\gamma) = c_i$ for $1 \le i \le n-1$. Then, by Lemma 3.2, γ has the Bruhat decomposition $\gamma = b_1cwb_2$, $b_1, b_2 \in \Gamma_\infty$ and, by Lemma 3.3, $M_\lambda(\gamma) = 0$ for $\lambda < \lambda_i$, $GCD(M_\lambda(\gamma)|\lambda \in L_i) = 1$ for $1 \le i \le n-1$, and $(M_\lambda(\gamma)|\lambda)$ satisfies the Plücker relations.

For each λ let $v_\lambda \equiv M_\lambda(\gamma) \bmod c_i$ be the least positive residue and let γ' be the Plücker inverse of v. This inverse exists because, by Lemma 3.5, the map $\gamma \to (M_\lambda(\gamma))$ is onto.

Then $c_i = M_{\lambda_i}(\gamma) = M_{\lambda_i'}(\gamma)$ because, by Lemma 3.4 the c_i are uniquely determined and $\gamma' = b_1'cwb_2'$. Since also $M_\lambda(\gamma') = v_\lambda \equiv M_\lambda(\gamma) \bmod c_i$ for $\lambda \in L_i$, by Lemma 3.5, the double cosets $\Gamma_\infty\gamma\Gamma_w = \Gamma_\infty\gamma'\Gamma_w$, so γ gives rise to a term in the computed sum.

2. Conversely, let (b_1, b_2) correspond to a term in the computed sum and let $\gamma = b_1cwb_2$, $b_1, b_2 \in \Gamma_\infty$. Then, by lemmas 3.3 and 3.5, $M_{\lambda_i}(\gamma) = c_i$, $M_\lambda(\gamma) = 0$ for $\lambda < \lambda_i, GCD(M_\lambda(\gamma)|\lambda \in L_i) = 1$ for $1 \le i \le n-1$, and, since they are the Plücker coordinates of a matrix, $(M_\lambda(\gamma)|\lambda)$ satisfies the Plücker relations. Hence there exists a vector $v \in \mathcal{V}''$ with $M_\lambda(\gamma) \equiv v_\lambda \bmod c_i$ which is invertible coming from a matrix a_v say, and, by Lemma 3.6, $\Gamma_\infty a_v\Gamma_w = \Gamma_\infty\gamma\Gamma_w$.

3. That each term in the computed sum corresponds to at most one double coset follows from Lemma 3.6. ∎

6. GL(N)PACK IMPLEMENTATION

The part of the GL(n)pack which treats Kloosterman sums consists of a number of user functions which can be used independently, as well as the primary function KloostermanSum. The Plücker relations are essential, and these are available through the function PluckerRelations. See the comments above and note that the algorithm which derives the sums is not dependent on the set of relations computed being "complete". The function PluckerCoordinates simply computes the bottom row based minors and PluckerInverse finds an integer matrix, when it exists, which has the given Plücker coordinates. This requires solving a system of linear integer equations for an integer unknown to determine each matrix row as described above.

Once a matrix is determined then its Bruhat decomposition is required. Even though the function KloostermanBruhatCell performs this step symbolically, a standard numeric Bruhat decomposition is performed, since the entries of the matrix a are only available as explicit integers. It is this step which prevents the algorithm from being fully symbolic. The existing examples in the literature in [2, 6] present answers in the form of expressions containing of the order of n^2 symbolic coefficients obeying constraints which must be determined to obtain an explicit solution.

Since these sums are only well defined for some particular compatible values of the arguments the user is advised to first run KloostermanCompatibility with an explicit w to determine those values. This function gives three types of information: any divisibility relations between the c_i's, constraints on the character coefficients, and constraints on the minors of the matrix a.

One thing to notice is the value returned by KloostermanSum. Even through the value is often set to 0 when the sum is invalid [6] the function returns False in this case. The value 0 is returned when the sum is well defined but has sum 0.

The complexity of the algorithm is $O(\prod_{1\le i\le n-1}|c_i|^n) = O(c^{n^2})$ where $c = \max|c_i|$, so its quite slow, especially for large c_is.

7. EXAMPLES FOR LOW DIMENSION

In [2] two types of Kloosterman sums appear for dimension $n = 3$. However, using the strategy described above, three non-trivial types are revealed: when $c_1 \mid 1$, when $c_2 \mid 1$, when $c_2 \mid c_1$ and when $c_1 \mid c_2$.

Example 7.1. In [6] an example for $n = 4$ is worked through by hand in some detail. This is for

$$w = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

and the divisibity relation $c_1 \mid c_2$ is derived. With the algorithm described here, the additional relation $c_3 \mid c_2$ is computed. Also note that in [6] a Bruhat decomposition $a = x.c.w.y$ is used which was derived "by hand" and assumed particular zero and non-zero values for some of the matrix elements. The GL (n)pack function KloostermanBruhatCell gives the following alternative values for the upper triangles of the unipotent matrixes x and y:

$$\begin{aligned}
x_{1,2} &\to \frac{a_{1,1}c_1(a_{3,2}a_{4,4} - a_{3,4}c_1) + (-a_{1,2}a_{4,4} + a_{1,4}c_1)c_2}{c_1c_3} \\
x_{1,3} &\to \frac{a_{1,1}c_1}{c_2} \\
x_{1,4} &\to \frac{a_{1,2}}{c_1} \\
x_{2,3} &\to \frac{a_{2,1}c_1}{c_2} \\
x_{2,4} &\to \frac{a_{2,2}}{c_1} \\
x_{3,4} &\to \frac{a_{3,2}}{c_1} \\
y_{1,2} &\to 0 \\
y_{1,3} &\to \frac{-a_{3,2}a_{4,3} + a_{3,3}c_1}{c_2} \\
y_{1,4} &\to \frac{-a_{3,2}a_{4,4} + a_{3,4}c_1}{c_2} \\
y_{2,3} &\to \frac{a_{4,3}}{c_1} \\
y_{2,4} &\to \frac{a_{4,4}}{c_1} \\
y_{3,4} &\to 0
\end{aligned}$$

Note that there is no division by elements of the matrix a, so zero values can be assumed. Verification that these rules give a correct decomposition (i.e. $a = x.c.w.y$) is a brute force computation which uses all of the constraints on the matrix a. It has been done for examples of particular w's in dimensions 3 and 4. The algorithm underlying this inversion was deduced by observing many cases of the right hand side and ascertaining their form.

Example 7.2. In [7, Page 175] an observation of Piatetski-Shapiro is noted that the only non-trivial sums, with all character coefficents non-zero, are those with corresponding w permutation matrices having a block structure with copies of the identity down the reverse leading diagonal. This was completely verified using KloostermanCompatibility in dimensions $n = 3$ and $n = 4$.

Example 7.3. Dimension 2: KloostermanSum[{24},{13},{43},LongElement[2]] returned the classical sum $S(24, 13; 43)$.

Example 7.4. Dimension 4: For the same Weyl group element w as that used in Example 7.1 above with character indices $\alpha = \{3, 7, 12\}, \beta = \{4, 13, 1\}$ and c values $\{3, 3, 3\}$ the sum $9e^{-\frac{2i\pi}{3}} + 8e^{\frac{2i\pi}{3}}$ was derived.

Example 7.5. By [7, Proposition 2.5] the long element sums should be commutative in the characters. this was verified in dimension 3 with kls[{3,13}, {6,7}, {3,3}, w0] and kls[{6,7}, {3,13}, {3,3}, w0] both returning $4 + 3e^{\frac{2i\pi}{3}} + 3e^{-\frac{2i\pi}{3}}$, kls being the abbreviated name for the function KloostermanSum and w0 the long element in dimension 3.

Example 7.6. By [7, Proposition 2.3] the value of each valid sum depends only on α_i mod c_{n-i} and β_i mod c_i. This was verified in dimension 3 with both kls[{4,13},{6,7}, {12,31}, w0] and kls[{35,25},{18,38},{12,31},w0] returning the same 60 term sum.

ACKNOWLEDGMENTS

I wish to gratefully acknowledge the assistance given by Dorian Goldfeld, Solomon Friedberg and Michael Eastwood in the preparation of this paper.

REFERENCES

1. K. Broughan, *The GL(n)pack manual.* Appendix to *Automorphic forms and L-functions for the group GL(n,R).* CUP. (to appear).
2. D. Bump, S. Friedberg and D. Goldfeld, *Poincaré series and Kloosterman sums for SL(3Z)*, Acta Arith. **50** (1988), p31-89.
3. D. Bump, S. Friedberg and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives.* Ann. Math. **131** (1990), p53-127.
4. J. -M. Deshouillers and H. Iwaniec, *Kloosterman sums and Fourier coefficients of cusp forms.*, Invent. Math. **70**, (1982) p219-288.
5. M. G. Eastwood and P. W. Michor, *Some Remarks on the Plücker relations*, (preprint).
6. S. Friedberg, *Explicit determination of GL(n) Kloosterman sums.* Séminaire de Théorie des Nombres de Bordeaux Année (1985-1986), p3-01 to p3-21.
7. S. Friedberg, *Poincaré Series for GL(n): Fourier expansion, Kloosterman sums and algebreo-geometric estimates.* Math. Z. **196** (1987), p165-188.
8. D. Goldfeld, *Automorphic forms and L-functions for the group GL(n,R).* CUP. (to appear).