Qubits and invariant theory

Ronald C King and Trevor A Welsh
School of Mathematics, University of Southampton, Southampton SO17 1BJ, England
E-mail: R.C.King@soton.ac.uk and taw@maths.soton.ac.uk

Abstract. The invariants of a mixed two-qubit system are discussed. These are polynomials in the elements of the corresponding density matrix. They are counted by means of group-theoretic branching rules and the Molien function is determined. The fundamental invariants are then explicitly constructed and the relations between them are found in the form of syzygies. In this way, complete sets of primary and secondary invariants are identified: there are 10 of the former and 15 of the latter.

1. Introduction
The entanglement of a two-qubit system is a non-local property so that measures of entanglement should be independent of all local transformations of the two qubits separately. Since a mixed two-qubit system is described by its density matrix, its non-local entangling properties must be described by local invariants of the density matrix. A complete set of local invariants is provided by local invariants that are homogeneous polynomials, that is polynomials of fixed total degree in the elements of the density matrix [1, 2].

It follows that there is a hierarchy of invariant theory problems relevant to a mixed two-qubit system. The first problem is to count the number of invariants \(n_m\) of a given degree \(m\) and to determine the corresponding generating function, that is to identify the Molien function \(M(q)\) whose power series expansion takes the form \(\sum_{m=0}^{\infty} n_m q^m\). The second problem is to construct the invariants explicitly, identifying a set of fundamental invariants, from which all others may be constructed as sums of products. By virtue of Hilbert’s Theorem [3], the cardinality of any set of fundamental invariants is known to be finite. The third problem is to determine the structure of the ring of invariants, which is necessarily Cohen-Macaulay [4]. To this end it is necessary to identify a set of primary invariants and a set of secondary invariants.

To state the problem more precisely, it should be noted that a single qubit is described by a quantum state \(\psi_i\) with two degrees of freedom specified by \(i = 0, 1\). A two-qubit system is then described by a linear superposition of direct product states \(\Psi_{a,i}(A, B) = \psi_a(A)\psi_i(B)\) with \(a, i = 0, 1\). For a mixed system the quantity of interest is the density matrix which takes the form

\[
\rho = \sum_{a,i,b,j=0}^{1} \rho_{a,i}^{b,j} \Psi_{a,i}(A) \Psi_j^*(B). \tag{1}
\]

Under arbitrary and independent non-singular local transformations of the two qubits defined
by
\[ g : \psi_i(A) \rightarrow \sum_{j=0}^{1} \psi_j(A) \ g_{ji} \quad \text{and} \quad h : \psi_a(B) \rightarrow \sum_{b=0}^{1} \psi_b(B) \ h_{ba} \]  
(2)

with \( g \times h \in GL_A(2) \times GL_B(2) \), the density matrix elements transform as
\[ g \times h : \rho_{a,b}^{c,d} \rightarrow \sum_{c,k,d,l} g_{ac} h_{ik} \rho_{d,l}^{c,k} g_{db}^{-1} h_{lj}^{-1}. \]  
(3)

With this notation, the task is first to count and then to construct all polynomial functions of the 16 components of \( \rho \) that are invariant under the local transformations \( g \times h \) of \( GL_A(2) \times GL_B(2) \), viewed as a subgroup of \( GL_{AB}(16) \).

2. Counting invariants

The 16 components, \( \rho_{a,b}^{c,d} \), of the mixed 2-qubit density matrix form the basis of the defining irreducible representation \( V \) of \( GL_{AB}(16) \). The homogeneous polynomials of degree \( m \) form the basis of the \( m \)th fold symmetrised power irreducible representation \( V^{(m)} \) of \( GL_{AB}(16) \). Let \( n_m \) be the number of linearly independent homogeneous polynomials that are invariant under the action of the local transformations of \( GL_A(2) \times GL_B(2) \). Then \( n_m \) is just the number of times the trivial, one-dimensional irreducible representation of \( GL_A(2) \times GL_B(2) \) appears in the restriction of \( V^{(m)} \) from \( GL_{AB}(16) \) to this subgroup.

Quite generally [5, 6], the polynomial irreducible representations of \( GL(n) \) have characters \( \{ \lambda \} \), specified by partitions \( \lambda \) of length \( \ell(\lambda) \leq n \), which are nothing other than Schur functions \( s_{\lambda}(x_1, \ldots, x_n) \) of the eigenvalues \( x_i \) of the group elements of \( GL(n) \). In addition there exist corresponding contragredient irreducible representations with characters \( \{ \bar{\lambda} \} \), which are Schur functions \( s_{\lambda}(x_1, \ldots, x_n) = x^{-1}_i \) of the inverse group elements.

We consider the following two group-subgroup chains from \( GL_{AB}(16) \) to \( GL_A(2) \times GL_B(2) \):

\[
GL_{AB}(16) \supset GL_A(4) \times GL_B(4) \\
\supset (GL_A(2) \times GL_A(2)) \times (GL_B(2) \times GL_B(2)) \\
\supset GL_A(2) \times GL_B(2); \tag{4}
\]

\[
GL_{AB}(16) \supset GL_{AB}(4) \times \overline{GL_{AB}(4)} \\
\supset (GL_A(2) \times GL_B(2)) \times (GL_A(2) \times GL_B(2)) \\
\supset GL_A(2) \times GL_B(2). \tag{5}
\]

The corresponding branching rules take the form [7]:
\[
\{ m \} \rightarrow \sum_{\lambda} \{ \lambda \} \times \{ \lambda \} \\
\rightarrow \sum_{\lambda,\mu,\nu,\sigma,\tau} \left( k_{\mu\nu}^{\lambda} \{ \mu \} \times \{ \nu \} \right) \times \left( k_{\sigma\tau}^{\lambda} \{ \sigma \} \times \{ \tau \} \right) \\
\rightarrow \sum_{\lambda,\mu,\nu,\sigma,\tau} \left( k_{\mu\nu}^{\lambda} k_{\sigma\tau}^{\lambda} \right) \left( + \cdots + \delta_{\mu\nu}\{0\} \right) \times \left( + \cdots + \delta_{\sigma\tau}\{0\} \right) \tag{6}
\]
and

\[ \{m\} \rightarrow \sum_{\lambda} \{\lambda\} \times \{\lambda\} \]

\[ \rightarrow \sum_{\lambda, \mu, \nu, \sigma, \tau} \left( k^\lambda_{\mu \nu} \{\mu\} \times \{\nu\} \right) \times \left( k^\lambda_{\sigma \tau} \{\sigma\} \times \{\tau\} \right) \]

\[ \rightarrow \sum_{\lambda, \mu, \nu, \sigma, \tau} k^\lambda_{\mu \nu} k^\lambda_{\sigma \tau} \left( + \cdots + \delta_{\mu \nu} \{0\} \right) \times \left( + \cdots + \delta_{\sigma \tau} \{0\} \right), \]  \hspace{1cm} (7)

where the coefficients \( k^\lambda_{\mu \nu} \) are defined by the inner product rule for characters of irreducible representations of the symmetric group \( S_m \), which takes the form:

\[ \chi^\mu_{\kappa} \chi^\nu_{\kappa} = \sum_{\lambda} k^\lambda_{\mu \nu} \chi^\lambda_{\kappa} \]. \hspace{1cm} (8)

In each of the two branching rules, \( \lambda, \mu, \nu, \sigma, \tau \) are partitions of \( m \), restricted by the conditions \( \ell(\lambda) \leq 4 \) and \( \ell(\mu), \ell(\nu), \ell(\sigma), \ell(\tau) \leq 2 \). These branching rules give rise to the following two formulae for the required multiplicities:

\[ n_m = \sum_{\lambda, \mu, \nu, \sigma, \tau} k^\lambda_{\mu \nu} k^\lambda_{\sigma \tau} \delta_{\mu \nu} \delta_{\sigma \tau} = \sum_{\lambda, m, \ell(\lambda) \leq 4} \left( \sum_{\mu, \ell(\mu) \leq 2} k^\lambda_{\mu \nu} \right)^2 \]  \hspace{1cm} (9)

\[ \sum_{\lambda, \mu, \nu, \sigma, \tau} k^\lambda_{\mu \nu} k^\lambda_{\sigma \tau} \delta_{\mu \nu} \delta_{\sigma \tau} = \sum_{\lambda, m, \ell(\lambda) \leq 4} \sum_{\mu, \nu, \ell(\mu), \ell(\nu) \leq 2} \left( k^\lambda_{\mu \nu} \right)^2. \]  \hspace{1cm} (10)

For example, in the case \( m = 4 \), we find that \( \lambda \) is to be summed over \( \{4\}, \{31\}, \{22\}, \{211\}, \{1111\} \). For each of these we have the branchings:

\[ \{4\} \rightarrow \{4\} \times \{4\} + \{31\} \times \{31\} + \{22\} \times \{22\}; \]

\[ \{31\} \rightarrow \{4\} \times \{31\} + \{31\} \times \{4\} + \{31\} \times \{31\} + \{31\} \times \{22\} + \{22\} \times \{22\}; \]

\[ \{22\} \rightarrow \{4\} \times \{22\} + \{31\} \times \{31\} + \{22\} \times \{4\} + \{22\} \times \{22\}; \]

\[ \{211\} \rightarrow \{31\} \times \{31\} + \{31\} \times \{22\} + \{22\} \times \{31\}; \]

\[ \{1111\} \rightarrow \{22\} \times \{22\}. \]

In the case of the first formula, for each \( \lambda \), we sum the coefficients of terms of the form \( \{\mu\} \times \{\mu\} \) and then sum the squares of these numbers to give \( n_4 = 3^2 + 1^2 + 2^2 + 1^2 + 1^2 = 16 \), while in the case of the second formula we sum the squares of all coefficients of \( \{\mu\} \times \{\nu\} \) to give \( n_4 = 16 \times 1^2 = 16 \).

Stimulated by the work of Davis et al [8, 9], Wybourne used his software package SCHUR [10] to carry out calculations of the above type and thereby to build up the corresponding Molien series term by term [11]:

\[ M(q) = \sum_{m=0}^{\infty} n_m \ q^m \]

\[ = 1 + q + 4q^2 + 6q^3 + 16q^4 + 23q^5 + 52q^6 + 77q^7 + 150q^8 + 224q^9 + 396q^{10} + 583q^{11} + 964q^{12} + 1395q^{13} + 2180q^{14} + 3100q^{15} + 4639q^{16} + 6466q^{17} + 9344q^{18} + 12785q^{19} + 17936q^{20} + 2412q^{21} + 33008q^{22} + 43674q^{23} + 58512q^{24} + 76277q^{25} + 100312q^{26} + 129009q^{27} + 166932q^{28} + 212022q^{29} + 270448q^{30} + O(q^{31}). \]  \hspace{1cm} (11)
Rather than extending this series by proceeding term by term, it is preferable to derive the corresponding generating function. To this end we can use Molien’s Theorem [3]. This states that if $G$ is a compact continuous group, with elements $g$ and Haar measure $d\mu(g)$, then

$$M(q) = \int_{g \in G} \frac{d\mu(g)}{\det(I - qg)}.$$  \hspace{1cm}(12)$$

In our case $G$ is in principle the non-compact group $GL_A(2) \times GL_B(2)$. However, the number of invariants is unchanged if we restrict from $GL_A(2) \times GL_B(2)$ to the compact subgroup $SU_A(2) \times SU_B(2)$. Moreover the invariants only arise from tensor products of pairs of irreducible representations and their contragredients of the form $\{\mu\} \times \{\nu\}$ and $\{\sigma\} \times \{\tau\}$. All the irreducible representations that appear in these products are faithful irreducible representations not of $SU_A(2) \times SU_B(2)$ but of $SO_A(3) \times SO_B(3)$. This allows us to take $G = SO_A(3) \times SO_B(3)$ with the group element $g$ corresponding to the 16-dimensional density matrix realised as the tensor product of two $4 \times 4$ matrices. This can be diagonalised to yield eigenvalues $\{1, e^{i\theta}, 1, e^{-i\theta}\} \times \{1, e^{i\phi}, 1, e^{-i\phi}\}$. The corresponding measure can be written in the form $d\mu(g) = (1 - \cos \theta)(1 - \cos \phi) \, d\theta \, d\phi$ [6]. Setting $z = e^{i\theta}$ and $w = e^{i\phi}$ then leads to integrations around $|z| = 1$ and $|w| = 1$. Molien’s Theorem then gives

$$M(q) = \oint_{|z|=1} \oint_{|w|=1} \frac{(1 - z)^2(1 - w)^2 z^{-2} w^{-1}}{(1 - q)(1 - qz)^2(1 - qz)^2}(1 - qw)^2(1 - q/w)^2 \, dw \, dz \, (1 - qz/w)(1 - qz/w)(1 - qw/z)(1 - qw/z).$$ \hspace{1cm}(13)$$

The repeated use of Cauchy’s residue theorem then yields

$$M(q) = \frac{1 - q^2 - q^3 + 2q^4 + 2q^5 + 2q^6 - q^7 - q^8 + q^{10}}{(1 - q)^{10}(1 + q)^6(1 + q^2)^2(1 + q + q^2)^3} \quad \frac{1 + q^4 + q^5 + 3q^6 + 2q^7 + 2q^8 + 3q^9 + q^{10} + q^{11} + q^{15}}{(1 - q)(1 - q^2)^2(1 - q^4)^2(1 - q^4)^3(1 - q^6)}.$$

$$\hspace{1cm}(14)$$

where the first form is due to Grassl et al [1], while the second emphasises the fact that, for $|q| < 1$, the expansion as a power series in $q$ yields a series in which all the coefficients $n_m$ are non-negative integers, as required.

3. Construction of the invariants

First we note some general properties of the ring $\mathcal{R}^G$ of invariants. Hilbert’s Theorem states that $\mathcal{R}^G$ is generated by a finite set of fundamental homogeneous invariants $\{I_1, I_2, \ldots, I_N\}$. The Cohen-Macaulay condition applies [4]. This states that there exists a set of primary invariants $K_m$ with $m = 1, 2, \ldots, n$ for some $n$ that are algebraically independent, and a set of secondary invariants $J_k$ with $k = 1, 2, \ldots, r$ for some $r$ that are linearly independent, such that

$$\mathcal{R}^G = \oplus_{k=0}^r J_k \mathbb{C}[K_1, K_2, \ldots, K_n],$$ \hspace{1cm}(15)$$

with $J_0 = 1$. This implies that an arbitrary invariant $I$ can always be expressed in the form $I = \sum_{k=0}^r J_k P_k(K_1, K_2, \ldots, K_n)$ with each $P_k$ polynomial in the $K_m$.

This general theory implies that the Molien function for $\mathcal{R}^G$ takes the form:

$$M(q) = \frac{\sum_{k=0}^r q^{|\deg J_k|}}{\prod_{m=1}^n (1 - q^{|\deg K_m|})}.$$ \hspace{1cm}(16)$$
Comparison with (14) then suggests, but does not prove, that in the mixed qubit case there are 10 primary invariants of degrees 1, 2, 2, 2, 3, 3, 4, 4, 4, and 15 secondary invariants of degrees 4, 5, 6, 6, 6, 7, 7, 8, 8, 9, 9, 9, 10, 11, 12.

To illustrate the fact that a knowledge of the Molien series generating function does not always determine the numbers and degrees of the primary and secondary invariants, consider the following example [12]. Let $G$ be the finite group generated by the matrices:

$$
\begin{pmatrix}
-1 & 0 & 0 \\
0 & -1 & 0 \\
0 & 0 & 1
\end{pmatrix},
\begin{pmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & i
\end{pmatrix}
$$

The Molien function of $G$ in this representation is given by:

$$M(q) = \frac{1}{(1 - q^2)^3}.$$

This suggests the existence of just 3 degree 2 primary invariants and no secondary invariants. However, if the space $V$ on which $G$ acts is spanned by vectors $v = (x, y, z)$, then $x^2, y^2, xy, z^4$ are fundamental invariants. Every homogeneous invariant is polynomial in these four. However, $(xy)^2 = x^2 y^2$, so that $xy$ is secondary and not primary. In fact the Molien function can be re-written in the form:

$$M(q) = \frac{1 + q^2}{(1 - q^2)^2(1 - q^2)},$$

corresponding to the fact that there are 3 primary invariants $x^2, y^2, z^4$ and 1 secondary invariant $xy$.

Our task is to identify the invariants and to confirm or otherwise the consistency of the Molien series (14) obtained by direct integration with the form (16) exhibiting the Cohen-Macaulay structure of the ring of invariants $\mathcal{R}^G$.

In order to exploit our knowledge of $SO(3)$ invariants, it is convenient to take advantage of the $SO_A(3) \times SO_B(3)$ structure of our problem by writing the two-qubit density matrix in the form [2]:

$$\rho = t \hat{I} \otimes \hat{I} + s_a \hat{\sigma}_a \otimes \hat{I} + p_i \hat{I} \otimes \hat{\sigma}_i + b_{ai} \hat{\sigma}_a \otimes \hat{\sigma}_i,$$

where $\hat{I}$ is the $2 \times 2$ unit matrix and $\hat{\sigma}_k$ for $k = 1, 2, 3$ are the Pauli matrices, and the repeated indices $a, i$ are summed over 1, 2, 3.

Then the aim is to construct $SO_A(3) \times SO_B(3)$ invariants as polynomials in the components of $t, s = (s_1, s_2, s_3), p = (p_1, p_2, p_3), b = (b_{ai})_{1 \leq a \leq 3}$ and $b^T = (b_{ai})_{1 \leq a \leq 3}$. In doing this, use may be made of the symmetric tensors $\delta_{ab}, \delta_{ij}$, and the antisymmetric tensors $\epsilon_{abc}, \epsilon_{ijk}$. The property characterising an invariant is that following contraction there must remain no free indices of either type, $a$ or $i$. A graphical approach to this problem is described elsewhere [13]. Here, following Makhlín [2], we summarise the outcome algebraically.

In accordance with the conjecture of Grassl et al [1], it is confirmed that there are just 21 fundamental invariants. Those involving no $\epsilon$ are:

$$K_1 := t, \quad K_6 := s_a b_{ai} p_i, \quad U_2 := s_a b_{ai} b_{aj} b_{bk} p_{i}p_{j}p_{k},$$

$$K_2 := b_{ai} b_{aj} p_{i}p_{j}, \quad K_7 := b_{ai} b_{aj} b_{bk} b_{bj} p_{i}p_{j}, \quad X_1 := s_a b_{ai} b_{aj} b_{bk} b_{bj} s_{c},$$

$$K_3 := s_a s_{a}, \quad K_8 := s_a b_{ai} b_{aj} b_{bk} b_{bj} s_{c}, \quad X_2 := p_i b_{ia} b_{ja} b_{kb} b_{kj} b_{bk} p_{k},$$

$$K_4 := p_i p_{i}, \quad K_9 := p_i b_{ia} b_{aj} p_{j}.$$ 

Those involving one $\epsilon$ are:

$$W_1 := \epsilon_{abc} s_a b_{ai} p_{i} b_{aj} b_{jd} b_{jd} s_{d}, \quad V_1 := \epsilon_{ijk} p_i b_{ja} b_{ja} s_{a} b_{ja} b_{ja} b_{jc} b_{jc} p_{l},$$

$$W_2 := \epsilon_{abc} s_a b_{aj} b_{ak} b_{ck} b_{ck} b_{ck} b_{cl} p_{l}, \quad V_2 := \epsilon_{ijk} p_i b_{ja} b_{ja} s_{a} b_{ja} b_{ja} b_{jc} b_{jc} p_{k},$$

$$W_3 := \epsilon_{ijk} p_i b_{ja} b_{ja} b_{ja} b_{kb} b_{kb} b_{kb} b_{mb} b_{mc} s_{c}, \quad V_3 := \epsilon_{abc} s_a b_{ja} b_{ja} b_{ja} b_{jc} b_{jc} b_{jc} b_{ck} b_{ck} p_{k},$$

$$W_4 := \epsilon_{ijk} p_i b_{ja} b_{ja} b_{ja} b_{kb} b_{kb} b_{kb} b_{mb} b_{mc} b_{cn} p_{n}, \quad V_4 := \epsilon_{abc} s_a b_{ja} b_{ja} b_{ja} b_{jc} b_{jc} b_{jc} b_{ck} b_{ck} b_{cf} b_{cf} p_{f}.$$
and those involving both $\epsilon s$ are
\[ K_5 := \det b = \frac{1}{b} \epsilon_{abc} \epsilon_{ijk} b_{ai} b_{bj} b_{ck} \quad U_3 := \epsilon_{abc} \epsilon_{ijk} s_a b_{bj} b_{ck} p_i. \]

Thus the fundamental invariants and their degrees are
\[
\begin{align*}
K_1 & : \text{deg } 1 & X_1, X_2, V_1, W_1 & : \text{deg } 6 \\
K_2, K_3, K_4, & : \text{deg } 2 & V_2, W_2 & : \text{deg } 7 \\
K_5, K_6 & : \text{deg } 3 & V_3, W_3 & : \text{deg } 8 \\
K_7, K_8, K_9, U_3 & : \text{deg } 4 & V_4, W_4 & : \text{deg } 9 \\
U_2 & : \text{deg } 5
\end{align*}
\]

The fact that there are no more fundamental invariants is discussed in detail elsewhere [13], but comes about through the existence of identities expressing every other homogeneous invariant as a polynomial in the above 21.

4. **Identification of primary and secondary invariants**

In order to identify and distinguish between primary and secondary invariants, the first step is to consider powers and products of the fundamental invariants and the relations between them, known as syzygies. A computer search reveals that there are 63 independent syzygies of the first kind. The invariants $K_m$ with $m = 1, 2, \ldots, 9$ are found to be algebraically independent and primary, while $U_i$, $V_j$ and $W_k$, with $i = 2, 3$ and $j, k = 1, 2, 3, 4$ are linearly independent but secondary by virtue of syzygies exemplified by:
\[
2 U_2^2 - 2 X_1 K_9 - 2 K_8 X_2 + 2 K_8 K_9 K_2 + K_6^2 K_7 - K_6^2 K_3^2 \\
-2 K_3 K_4 K_2^2 + 2 U_3 K_5 K_6 = 0; \\
U_3^2 + 8 K_6 U_2 - 4 K_6^2 K_2 - 4 K_8 K_9 + 4 K_3 K_9 K_2 + 4 K_8 K_4 K_2 \\
+2 K_3 K_4 K_7 - 2 K_3 K_4 K_2^2 - 4 X_1 K_4 - 4 K_3 X_2 = 0.
\]

There exists no similar expansion involving a term $U_2 U_3$, however $U_i V_j$ and $U_i W_j$ can be eliminated by means of syzygies such as:
\[
2 U_2 V_3 - W_1 K_6 K_7 + W_1 K_6 K_2^2 - 2 V_4 K_9 \\
-2 K_5 V_1 K_8 + 4 K_3 V_2 K_6 - 2 K_5 W_3 K_3 = 0; \\
U_3 W_2 + 2 V_1 K_6 K_2 - 2 V_2 K_9 + 4 W_3 K_6 - 2 W_4 K_3 - 2 K_5 W_1 K_4 = 0.
\]

All $V_i^2$, $W_j^2$ and $V_i W_j$ may be eliminated in the same way, as can all $W_k X_1$ and $V_k X_2$ by means of syzygies such as:
\[
W_1 X_1 - W_1 K_8 K_2 - V_3 K_8 + V_4 K_6 - K_3 V_2 K_3 = 0; \\
V_1 X_2 - V_1 K_9 K_2 - W_3 K_9 + W_4 K_6 - K_5 W_2 K_4 = 0.
\]

The same is not true of any $W_k X_2$ or $V_k X_1$, nor of $X_i^2$ or $X_j^2$; none of which can be eliminated in this way. However, the elimination of $X_1 X_2$ proceeds by way of the syzygy:
\[
2 X_1 X_2 - 2 X_1 K_9 K_2 - 2 K_8 X_2 K_2 + K_8 K_9 K_7 \\
+ K_8 K_9 K_2^2 - 2 U_2 K_6 K_7 + 2 U_2 K_6 K_2^2 + K_6^2 K_7 K_2 \\
- K_6^2 K_3^2 - 2 U_3 K_5 K_6 K_2 - 2 K_6^2 K_3^2 \\
+ 2 K_8 K_4 K_5^2 + 2 K_3 K_9 K_5^2 - 2 K_3 K_4 K_5^2 K_2 = 0, \quad (18)
\]
where it has been convenient to introduce $U_4 := U_2 U_3$.

Now let

$$D := \prod_{m=1}^{9} (1 - K_m),$$

$$U := 1 + \sum_{i=2}^{4} U_i, \quad V := \sum_{i=1}^{4} V_i, \quad W := \sum_{i=1}^{4} W_i.$$ 

Then, taking all syzygies into account, the generating function for polynomial invariants takes the form:

$$F := \frac{1}{D} \left( U + \frac{U X_1}{1 - X_1} + \frac{U X_2}{1 - X_2} + \frac{V}{1 - X_1} + \frac{W}{1 - X_2} \right),$$

in the sense that every linearly independent homogeneous invariant appears once and once only in the formal expansion of $F$.

As a check on the validity of this generating function, it is found that replacing each invariant $I$ in (19) by $q^{\deg(I)}$ leads directly to the formula (14) for the Molien function $M(q)$, as required.

The fact that both $X_1$ and $X_2$ cannot be algebraically independent of one another and of $K_m$ for $m = 1, 2, \ldots, 9$ comes about from the existence of a syzygy linking just $X_1, X_2$ and all these $K_m$. It is about 10 pages long and is of degree 48. Its dependence on $X_1$ and $X_2$ is illustrated by setting $K_m = z^{\deg(K_m)}$ for $m = 1, 2, \ldots, 9$ which gives:

$$16 X_1^4 X_2^4 + 8832 z^{36} X_1 X_2 - 7040 X_1^2 X_2^2 z^{30}$$
$$- 2112 z^{30} X_2^2 + 144 z^{24} X_1^4 - 2112 z^{30} X_3^3 - 1088 z^{42} X_1$$
$$+ 1984 X_1^2 X_2^2 z^{24} + 128 z^{24} X_1^3 X_2 - 1088 z^{42} X_2$$
$$+ 144 z^{24} X_2^4 + 896 X_1^3 z^{18} X_2^2 + 6496 z^{36} X_2^2$$
$$- 7040 z^{30} X_2^2 X_1 - 32 z^{12} X_1^4 X_2 - 64 X_1^4 X_2^3 z^{6}$$
$$+ 192 z^{18} X_1^4 X_2 + 128 X_1^3 X_2^2 z^{24} - 32 z^{12} X_2^4 X_1^2$$
$$+ 896 X_1^2 X_2^2 z^{18} - 6512 z^{48} + 192 z^{18} X_2^4 X_1$$
$$- 384 X_1^4 X_2^3 z^{12} + 6496 z^{36} X_1^2 - 64 z^{6} X_2^4 X_1 = 0.$$ 

This implies that $X_1$ and $X_2$ cannot both be primary invariants. However, in our expansion of $F$ in (19) it is clear that arbitrarily large powers of both $X_1$ and $X_2$ occur. The way out of this apparent impasse is to define $K_{10} := X_1 + X_2$ and $J_3 := X_1 - X_2$. Then $K_m$ for $m = 1, 2, \ldots, 10$ are algebraically independent. Moreover $J_3^2 = K_{10}^2 - 4 X_1 X_2$ with $X_1 X_2$ known to be linear in $X_1, X_2, U_2, U_3, U_4$ from (18). This is sufficient to conclude that $J_3^2$ is linear in $J_3, U_2, U_3, U_4$, with coefficients polynomial in $K_1, K_2, \ldots, K_{10}$, and can be eliminated.

It follows that our primary and secondary invariants and their degrees can be identified as follows: the 10 primary invariants:

$$K_1 \quad \text{deg} 1$$
$$K_2, K_3, K_4 \quad \text{deg} 2$$
$$K_5, K_6 \quad \text{deg} 3$$
$$K_7, K_8, K_9 \quad \text{deg} 4$$
$$K_{10} = X_1 + X_2 \quad \text{deg} 6.$$
and the 15 secondary invariants:

\[
\begin{align*}
J_1 &:= U_3 \quad \text{deg 4} & J_8, J_9 &:= V_1, W_1 \quad \text{deg 6} \\
J_2 &:= U_2 \quad \text{deg 5} & J_{10}, J_{11} &:= V_2, W_2 \quad \text{deg 7} \\
J_3 &:= X_1 - X_2 \quad \text{deg 6} & J_{12}, J_{13} &:= V_3, W_4 \quad \text{deg 8} \\
J_4 &:= J_1 J_2 \quad \text{deg 9} & J_{14}, J_{15} &:= V_4, W_4 \quad \text{deg 9} \\
J_5 &:= J_1 J_3 \quad \text{deg 10} \\
J_6 &:= J_2 J_3 \quad \text{deg 11} \\
J_7 &:= J_1 J_2 J_3 \quad \text{deg 15}
\end{align*}
\]

5. Conclusion
Recalling that \( J_0 = 1 \), the ring \( \mathcal{R}^G \) of invariants takes the Cohen-Macaulay form:

\[
\mathcal{R}^G = \bigoplus_{k=0}^{15} J_k \mathbb{C}[K_1, K_2, \ldots, K_{10}].
\]

The Molien series for \( \mathcal{R}^G \) is given by

\[
M(q) = \frac{\sum_{k=0}^{15} q^{\deg J_k}}{\prod_{m=1}^{10} (1 - q^{\deg K_m})}
\]

with 10 primary invariants \( K_m \) of degrees 1, 2, 2, 2, 3, 3, 4, 4, 4, 6, and 15 secondary invariants \( J_k \) of degrees 4, 5, 6, 6, 7, 7, 8, 8, 9, 9, 9, 10, 11, 15.

Acknowledgments
It is a pleasure to thank Professor C J Cummins of Concordia University, Montreal for some helpful suggestions given to one of us (RCK) regarding the search for syzygies using Maple. One of us (RCK) is grateful for the award of a Leverhulme Emeritus Fellowship which enabled him to offer partial support to the other (TAW).

References
[1] Grassl M, Rotteler M and Beth T 1998 Computing local invariants of qubit quantum systems Phys. Rev. A 58 1833–1839
[2] Makhlin Y 2002 Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations Quantum Info. Proc. 1 243–252
[3] Sturmfels B 1993 Algorithms in Invariant Theory (Wien: Springer)
[4] Hochster M and Roberts J 1974 Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay Adv. Math. 13 115–175
[5] Weyl H 1946 The Classical Groups (Princeton, NJ: Princeton Univ. Press)
[6] Littlewood D E 1950 The Theory of Group Characters 2nd Ed. (Oxford: Clarendon Press)
[7] King R C 1975 Branching rules for classical Lie groups using tensor and spinor methods J. Phys. A 8 429–449
[8] Davis R I A, Delbourgo R and Jarvis P D 2000 Covariance, correlation and entanglement J. Phys. A 33 1895–1914
[9] Davis R I A, Delbourgo R and Jarvis P D 2000 Integrity bases for local invariants of composite quantum systems J. Phys. A 33 3723–3725
[10] Wybourne B G 1990 SCHUR: An Interactive Programme for Calculating Properties of Lie Groups http://smc.vnet.net/schur.html
[11] Wybourne B G 2000 Private communication
[12] Stanley R P 1979 Invariants of finite groups and their applications to combinatorics Bull. Amer. Math. Soc. 1 475–511
[13] Welsh T A, Jarvis P D and King R C to appear Invariants of mixed qubit systems, in Proceedings of the Brian G Wybourne Commemorative Meeting Eds: King R C, Karwowski J and Bylicki M (Toruń, Poland: Nicolaus Copernicus University Press)