# THE FORMAL MODULAR INVARIANT THEORY OF BINARY QUANTICS*

BY

O. E. GLENN

The group, $G$, represented by the general binary linear transformation in which the coefficients are parameters representing residues of the prime number $p$, has the universal covariants†

$$L_t = x_1^{p^t} x_2 - x_1 x_2^{p^t},$$

a fundamental system being given by $L = L_1$, $Q = L_2/L_1$. Assume that

$$f_m = (a_0, a_1, \cdots, a_m \between x_1, x_2)^m$$

is a binary quantic of order $m$ whose coefficients are variables. We study the functions of the $a$'s and $x$'s which are invariantive under the operation of transforming $f_m$ by $G$. Sections 1, 2, 3 deal with methods of constructing such functions, especial attention being given to the case $p = 2$. In § 5 fundamental systems of first degree concomitants of the quartic and quintic are derived. Section 4 is devoted to a proof that if the systems of concomitants modulo 2 of the forms of orders $1, 2, 3$ and the simultaneous systems obtained by combining forms of these three orders are all finite, then the system of $f_m$ is likewise finite. The hitherto undemonstrated theorem on the finiteness of the formal concomitants modulo 2 is thus reduced to a comparatively simple problem. In § 6 there is proved a theorem on the reducibility of any covariant, modulo 2, of the binary cubic in terms of a set of fourteen invariants and covariants.

## 1. Invariant operators

In addition to modular polars and transvectants previously discussed‡ by the present writer we cite, in order to augment the number of construction

* Presented to the Society, February 26, 1916.

† Dickson, these Transactions, vol. 12 (1911), p. 75; and *Madison Colloquium Lectures*, 1913, p. 33.

‡ O. E. Glenn, American Journal of Mathematics, vol. 37 (1915), p. 73; and Bulletin of the American Mathematical Society, vol. 21 (1915), p. 167.

methods, the universal operators obtained by replacing, in $L$ and $Q$, the variables $x_1$, $x_2$ by the cogredient elements $\partial/\partial x_2$, $-\partial/\partial x_1$. Call these operators respectively $L_\delta$ and $Q_\delta$;

$$Q_\delta = \frac{\partial^{p(p-1)}}{\partial x_1^{p(p-1)}} + \frac{\partial^{p(p-1)}}{\partial x_1^{(p-1)(p-1)}\,\partial x_2^{p-1}} + \cdots .$$

If $K_M$ is any formal covariant modulo $p$ of degree-order $(i, M)$ and if

$$(p+1)r + p(p-1)s + w = M, \tag{1}$$

then

$$C_{rsw} = L_\delta^r\, Q_\delta^s\, K_M$$

is a formal covariant of degree-order $(i, w)$. The number of concomitants yielded by this formula equals the number of distinct solutions in positive integers $(r, s, w)$ of the linear diophantine equation (1). The lists given below are for $p = 2$, $K_M \equiv f_m$, each giving all forms $C_{rsw}$ for the corresponding $m$. Corresponding to each invariant $C_{rs0}$ there exists an invariant operator $\sum(\partial/\partial a)$ obtained by constructing the Aronhold operator for the two forms $L^r Q^s, f_m$. These are also given in the particular cases shown.

$$m = 4$$

$$C_{020} = a_1 + a_2 + a_3; \qquad \frac{\partial}{\partial a_0} + \frac{\partial}{\partial a_2} + \frac{\partial}{\partial a_4},$$

$$C_{101} = a_1 x_1 + a_3 x_2, \qquad C_{012} = a_1 x_1^2 + a_3 x_2^2.$$

$$m = 5$$

$$C_{110} = a_1 + a_2 + a_3 + a_4; \qquad \frac{\partial}{\partial a_1} + \frac{\partial}{\partial a_4},$$

$$C_{021} = a_2 x_1 + a_3 x_2, \qquad C_{102} = a_2 x_1^2 + a_3 x_2^2, \qquad C_{013} = QC_{021}.$$

$$m = 6$$

$$C_{200} = C_{030} = a_3; \qquad \frac{\partial}{\partial a_0} + \frac{\partial}{\partial a_1} + \frac{\partial}{\partial a_3} + \frac{\partial}{\partial a_5} + \frac{\partial}{\partial a_6}; \qquad \frac{\partial}{\partial a_2} + \frac{\partial}{\partial a_4},$$

$$C_{111} = (a_1 + a_3)x_1 + (a_3 + a_5)x_2, \qquad C_{022} = a_3 Q, \qquad C_{103} = a_3 L,$$

$$C_{014} = a_1 x_1^4 + a_3 x_1^2 x_2^2 + a_5 x_2^4.$$

$$m = 7$$

$$C_{120} = a_1 + a_2 + a_3 + a_4 + a_5 + a_6; \qquad \sum_{i=1}^{6} \frac{\partial}{\partial a_i},$$

$$C_{201} = (a_2 + a_4)x_1 + (a_3 + a_5)x_2,$$

$$C_{031} = (a_0 + a_1 + a_3 + a_5 + a_6)x_1 + (a_1 + a_2 + a_4 + a_6 + a_7)x_2,$$

$$C_{112} = (a_1 + a_4)x_1^2 + (a_3 + a_6)x_2^2,$$

$$C_{023} = (a_0 + a_2 + a_4)x_1^3 + (a_1 + a_3 + a_5)x_1^2 x_2 + (a_2 + a_4 + a_6)x_1 x_2^2 + (a_3 + a_5 + a_7)x_2^3,$$

$$C_{104} = (a_1 + a_2)x_1^4 + (a_5 + a_6)x_2^4,$$

$$C_{015} = (a_0 + a_1 + a_2)x_1^5 + (a_1 + a_2 + a_3)x_1^4 x_2 + (a_4 + a_5 + a_6)x_1 x_2^4 + (a_5 + a_6 + a_7)x_2^5.$$

## 2. Covariants led by assigned seminvariants

If we add to the variables $a_0, a_1, \cdots; x_1, x_2$ in any formal covariant $\phi(a_0, \cdots; x_1, x_2)$ of $f_m$ the increments of these variables when $f_m$ is transformed by $x_1 = x_1', x_2 = tx_1' + x_2'$, and then expand $\phi(a_0 + \delta a_0, \cdots)$ by Taylor's theorem, we find that any formal covariant modulo $p$ has an annihilator of the type*

$$\Upsilon = O_0 + O_1 x_1 \frac{\partial}{\partial x_2} + O_2 x_1^2 \frac{\partial^2}{\partial x_2^2} + \cdots + O_j x_1^j \frac{\partial^j}{\partial x_2^j} + \cdots.$$

In this theory $t$ is any residue modulo $p$ and the expansion in question contains only the $p$ terms obtained by reducing all powers of $t$ below the $p$th by Fermat's theorem. The operator $O_j$ $(j = 0, 1, \cdots)$ is a partial differential operator in the derivatives with respect to the coefficients of $f_m$, non-homogeneous as to the derivatives the orders of which range from zero to infinity in each $O_j$.

If we apply $\Upsilon$ to a covariant and proceed as in the well-known proof of Roberts' theorem on the unique determination of an algebraical covariant from its seminvariant leader we find that the resulting relations in the covariant's coefficients and the operators $O_j$ $(j = 0, 1, \cdots)$ are not recurrent in the formal theory, whereas they are recurrent in the algebraic theory. Thus a formal covariant is not uniquely determined from its leader. This is also evident from the fact that if $T$ is any such covariant of order $w \not\equiv 0 \pmod{p}$, then

$$\left( x_1^p \frac{\partial}{\partial x_1} + x_2^p \frac{\partial}{\partial x_2} \right) T$$

is also a formal covariant having the same seminvariant leader.

Under definite conditions we can, however, derive a covariant $T$ of order $p - 1$ of $f_m$ having a given seminvariant $S$ as leader. This is done by substituting for $a_0, a_1, a_2, \cdots$ in $S$ the derivatives

* Cf. Dickson, these Transactions, vol. 8 (1907), p. 209. An explicit $\Omega_0(\delta)$, analogous to $O_0$, is given in my paper in American Journal of Mathematics, loc. cit., p. 75.

$$f_m, \quad \frac{1}{m}\frac{\partial f_m}{\partial x_2}, \quad \frac{1}{m(m-1)}\frac{\partial^2 f_m}{\partial x_2^2}, \cdots,$$

regarding $x_1$, $x_2$ as integers modulo $p$ and rearranging the result as a polynomial in $x_1$, $x_2$ of order $p-1$. This is analogous to the process of Faà di Bruno for algebraic covariants. The same result is reached by expanding $S(a_0', a_1', \cdots)$, corresponding to the transformation of $f_m$ by

$$x_1 = x_1', \qquad x_2 = tx_1' + x_2',$$

replacing $t$ by $x_2/x_1$ and multiplying by $x_1^{p-1}$. The result is

$$T = Sx_1^{p-1} + \frac{O_0 S}{\lfloor 1}x_1^{p-2}x_2 + \cdots + \frac{O_0^{p-1}S}{\lfloor p-1}x_2^{p-1}. \tag{2}$$

This is a formal covariant only provided it satisfies the differential congruence $\Upsilon T \equiv 0 \pmod{p}$, and is symmetrical under the substitution

$$s = (a_0 a_m)(a_1 a_{m-1}) \cdots (x_1 x_2).$$

Imposing these conditions we deduce the conditions which $S$ must satisfy in order that it may lead the covariant of order $p-1$. These are, (*a*) that $S$ should be transformed into $O_0^{p-1}S/\lfloor p-1$ by $s$, and (*b*) that the following congruences should be satisfied:

$$\left.\begin{aligned}
&O_0^p S \equiv 0,\\
&(O_0^{p-1} + O_1 O_0^{p-1})S \equiv 0,\\
&(O_0^{p-2} + O_1 O_0^{p-2} + O_2 O_0^{p-1})S \equiv 0,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&(O_0^2 + O_1 O_0^2 + O_2 O_0^3 + \cdots + O_{p-2}O_0^{p-1})S \equiv 0,\\
&(O_0 + O_1 O_0 + O_2 O_0^2 + \cdots + O_{p-1}O_0^{p-1})S \equiv 0.
\end{aligned}\right\} \pmod{p}, \tag{3}$$

The theory of $T$ is thus complicated. It is given here because nothing has been published hitherto on the determination of a covariant with a given leader, and also for the reason that it is of much practical use in constructing covariants with assigned properties in special cases. Let $p = 2$, $m = 3$. A seminvariant of $f_3$ is $S = a_0 a_2 + a_1^2$. Transformation of $f_3$ by $x_1 = x_1'$, $x_2 = tx_1' + x_2'$ gives

$$\begin{aligned}
S' &\equiv [a_0 + t(a_1 + a_2 + a_3)](a_2 + ta_3) + (a_1 + ta_3)^2\\
&\equiv a_0 a_2 + a_1^2 + (a_0 a_3 + a_1 a_2 + a_1 a_3 + a_2^2)t \pmod{2}.
\end{aligned}$$

Rendering $S$ symmetrical with the coefficient of $t$ (condition (*a*)) by adding the invariant $a_0 a_3 + a_1 a_2 = \Delta$, (annihilated by $O_0$) we have the formal linear covariant*

* Cf. American Journal of Mathematics, loc. cit., p. 78.

$$C_1^{(2)} = (S + \Delta)x_1 + (\Delta + a_1 a_3 + a_2^2)x_2 .$$

For $p = 3$, $m = 2$, $S = a_0 a_1^3 - a_0^3 a_1$, the method leads easily to the quadratic covariant of $f_2$,

$$C_6 = Sx_1^2 + (a_0 a_2^3 - a_0^3 a_2)x_1 x_2 + (a_1 a_2^3 - a_1^3 a_2)x_2^2 .$$

## 3. Some covariants of $f_m$ modulo 2

For the modulus 2 the real points $(x_1, x_2)$, other than $(0, 0)$, in the plane are $(1, 1)$, $(0, 1)$, $(1, 0)$. The values of $f_m$ at these points are, respectively,

$$a_0 + a_1 + \cdots + a_m , \qquad a_m , \qquad a_0 .$$

By a theorem* of Dickson's, any symmetric function of these three expressions is a formal invariant, modulo 2, all such being, of course, rational in the three elementary symmetric functions

$$(4) \qquad \begin{gathered} K = a_1 + a_2 + \cdots + a_{m-1} , \qquad I = a_0 a_m + (a_0 + a_m)(a_0 + a_m + K), \\ k = a_0(a_0 + K + a_m)a_m . \end{gathered}$$

In the same way if

$$C_M = A_0 x_1^M + A_1 x_1^{M-1} x_2 + \cdots$$

is any formal covariant of $f_m$, modulo 2, any symmetric function of

$$A_0 + \cdots + A_M , \qquad A_0 , \qquad A_M$$

is an invariant of the original form $f_m$. Thus the middle coefficient of any quadratic covariant of $f_m$ is an invariant, the sum of the two middle coefficients of any cubic covariant is an invariant, and so on.

By means of the transformations on the $a$'s induced by $x_1 = x_1' + tx_2'$, $x_2 = x_2'$, viz.

$$(5) \qquad a_r' = \left[ \binom{m}{r} a_0 + \binom{m-1}{r-1} a_1 + \cdots + \binom{m-r+1}{1} a_{r-1} \right] t + a_r \qquad (r = 0, \cdots, m),$$

it is readily shown that

$$(5_1) \qquad K_2 = a_0 x_1^2 + Kx_1 x_2 + a_m x_2^2 , \qquad K_1 = (a_0 + K)x_1 + (K + a_m)x_2 ,$$

are formal covariants modulo 2.

Lemma. *For any odd order $m > 1$ ($p = 2$) the form $f_m$ has a cubic covariant $K_{m3}$ with leading coefficient $a_0$, which is such that*

$$K_{m3} \equiv K_2 \qquad (\mathrm{mod}\ 2)$$

*for integral values of $x_1$, $x_2$.*

* These Transactions, vol. 15 (1914), p. 497.

The covariants $K_{m3}$ for the first twelve odd orders $m$ are

$$K_{33} = a_0 x_1^3 + a_1 x_1^2 x_2 + a_2 x_1 x_2^2 + a_3 x_2^3,$$

$$K_{53} = a_0 x_1^3 + (a_1 + a_2) x_1^2 x_2 + (a_3 + a_4) x_1 x_2^2 + a_5 x_2^3,$$

$$K_{73} = a_0 x_1^3 + (a_1 + a_2 + a_4) x_1^2 x_2 + (a_3 + a_5 + a_6) x_1 x_2^2 + a_7 x_2^3,$$

$$K_{93} = a_0 x_1^3 + (a_1 + a_2 + a_3 + a_4) x_1^2 x_2 + (a_5 + a_6 + a_7 + a_8) x_1 x_2^2 + a_9 x_2^3,$$

$$K_{113} = a_0 x_1^3 + (a_1 + a_2 + a_4 + a_5 + a_8) x_1^2 x_2 + (a_3 + a_6 + a_7 + a_9 + a_{10}) x_1 x_2^2 + a_{11} x_2^3.$$

The general form to be proved is

$$K_{m3} = a_0 x_1^3 + I_1 x_1^2 x_2 + I_2 x_1 x_2^2 + a_m x_2^3,$$

where

$$I_1 = a_{i_1} + \cdots + a_{i_s}, \qquad I_2 = a_{j_1} + \cdots + a_{j_s}, \qquad s = \tfrac{1}{2}(m-1),$$

$$I_1 + I_2 = K.$$

Assuming the increments of $I_1$, $I_2$ under (5) to be $I_1' t$, $I_2' t$ we readily show that

$$I_1' \equiv I_2' \equiv a_0 \pmod 2.$$

Hence, letting $I_1 = \alpha_1 a_1 + \cdots + \alpha_{m-1} a_{m-1}$ $(\alpha_j = 0 \text{ or } 1)$, we have from $\sum_{r=1}^{r=m-1} \alpha_r a_r'$, with (5), the conclusion that the selection of the set $a_{i_1}, a_{i_2}, \cdots, a_{i_s}$ is accomplished by selecting a set $\sigma_1$ of columns from the following Pascal triangle (6), the set to have the properties (*a*), (*b*) below:

$$
(6)\qquad
\begin{array}{cccccc}
 & & & & & \binom{2}{1}, \\
 & & & & \binom{3}{1} & \binom{3}{2}, \\
\cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot \\
 & \binom{m-1}{1} & \binom{m-1}{2} & \cdots & \binom{m-1}{m-3} & \binom{m-1}{m-2}, \\
\binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & \binom{m}{m-2} & \binom{m}{m-1}, \\
a_1 & a_2 & a_3 & \cdots & a_{m-2} & a_{m-1}.
\end{array}
$$

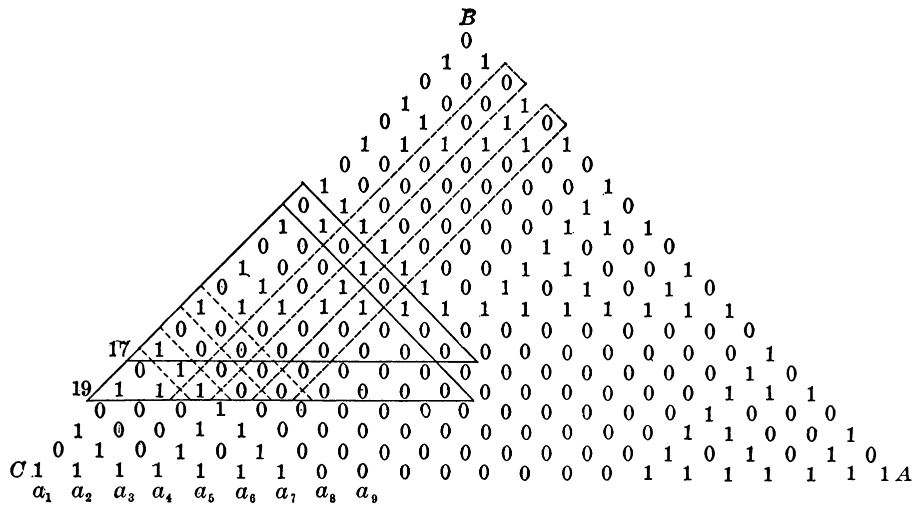
(*a*) The sum of the numbers of the first row of the selected set $\sigma_1$ is odd.

(*b*) The sum for all of the other rows of $\sigma_1$ is even.

Grant for the moment that such a set can be selected. If its columns be deleted from (6) the set $\sigma_2$ of columns remaining in (6) will also have the properties (*a*), (*b*) since Pascal's triangle is symmetrical with respect to the median drawn from $\binom{2}{1}$. This second set $\sigma_2$ gives $a_{j_1}, a_{j_2}, \cdots, a_{j_s}$, i. e., $I_2$.

We now construct the triangle $ABC$ made up of the residues modulo 2 of

Pascal's triangle, placing $\binom{2}{1}$ at the upper vertex, with the aforesaid median drawn vertically. We note particularly the symmetrical properties, and in particular the regular recurrence of the inverted triangles of zeros, of increasing dimensions, having the median as a line of symmetry. Consider any element $e$ of any horizontal row, to the left of the median. We call the column parallel to $AB$ and containing $e$ the column of $e$. The element $e'$ in the same row as $e$ but occupying the complementary position to the right of the median is called the complementary element of $e$. The column parallel to $AB$ containing $e'$ is the complementary row of $e$, and the column containing $e$ and parallel to $BC$ is the complementary column of $e$. We have $e' = e$, and the complementary row and complementary column of $e$ identical.




Suppose we wish to select $I_1$, i. e., the set $\sigma_1$, for $m = 19$. We take the left-hand half-row number 18 from $B$ as hypotenuse and draw the triangle enclosing the columns of these elements. The elements on the hypotenuse correspond to set

$$T_1 : a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9.$$

If the rows enclosed within this triangle satisfy conditions ($a$), ($b$) (as is the case for $m = 17$) then $\sigma_1$ would be the set $T_1$ and $I_1$ equal to the sum of the $\frac{1}{2}(m - 1)a$'s in their natural order beginning with $a_1$. The sums of the rows above the first in the triangle are however $1, 1, 0, 1, 0, 1, 0, 1 \pmod 2$ respectively, instead of $0, 0, 0, 0, 0, 0, 0, 0 \pmod 2$ required by condition ($b$). To secure a triangle (augmented) which does satisfy ($b$) we replace some of the elements on the hypotenuse by their complementary elements, in this case $e_3, e_5$ (corresponding to $a_3, a_5$) by $e_3', e_5'$ (corresponding to $a_{16}, a_{14}$).

The columns of $e_3$, $e_5$ are thus replaced by their complementary columns by rotating the latter counter-clockwise around $e_3$, $e_5$. The augmented triangle now satisfies conditions (*a*), (*b*) and hence

$$I_1 = a_1 + a_2 + a_{16} + a_4 + a_{14} + a_6 + a_7 + a_8 + a_9.$$

Now the orders $m$ for which the triangles do not need to be augmented are those giving the first row below the base of each central triangle of zeros. These values of $m$ are

$$(7) \qquad 3,\ 5,\ 9,\ 17,\ 33,\ \cdots,\ 2^n + 1,\ \cdots$$

and $2^n - 1$ is the number of the row, counting downward from $B$, in which the base of the $n$th central triangle of zeros is found. For $m = 2^n + 1$, $I_1$ equals the sum of the first $2^{n-1}$ $a$'s in their natural order, $I_1 = a_1 + a_2 + \cdots$. Between any two consecutive cases of (7) there is a cycle of augmented triangles such that the whole configuration from $B$ downward forms a sequence of recurring cycles of figures proceeding according to the laws of symmetry of the triangle $ABC$. Thus the set $\sigma_1$ can always be selected and the lemma is true.

We now observe that any covariant $C_M$ of $f_m$ of odd order $M$ has corresponding to it a quadratic and a cubic covariant of $f_m$, constructed as covariants of $C_M$, on the models of $K_2$, $K_{m3}$ respectively. (Cf. § 6.)

## 4. The finiteness of the formal concomitants for the order $m$ and modulus 2

Theorem. *The general quantic $f_m$, $m > 3$, is reducible, modulo 2, in terms of $Q$, $L$, and its own covariants of the first degree and orders* 1, 2, 3.

Let $m$ be even, $m = 2k$. Then $f_m - Q^{k-1} K_2$ has the factor $x_2$. Hence it has the factor $L$, since the real points (mod 2) form a conjugate set under the group $G$. Therefore

$$(8) \qquad f_m \equiv Q^{k-1} K_2 + LC \qquad (\text{mod } 2),$$

where $C$ is a first degree covariant of $f_m$ of odd order $2k - 3$. Next let $m$ be odd, $m = 2h + 3 > 3$. Then

$$(9) \qquad f_m \equiv Q^h K_{m3} + LC' \qquad (\text{mod } 2),$$

where $C'$ is of even order $2h$.

The forms $C$, $C'$ are, in turn, reducible in terms of their own covariants of orders 2, 3 with $L$ and $Q$, and, as a covariant of $C$ is a covariant of $f_m$, we are led to a recurring process by which $f_m$ is in all cases expressed in terms of its covariants of orders 1, 2, 3, and $L$ and $Q$, which was to be proved.

Any concomitant of a polynomial in a set of concomitants is a function of concomitants of the forms in the set. Hence if the systems for the orders $1, 2, 3$, and the simultaneous systems modulo 2 for these three orders are finite, the system for $f_m$ is likewise finite (see § 6).

## 5. Systems of the first degree

While illustrating formulas (8), (9), we now derive fundamental systems of first degree concomitants for the quartic and the quintic forms.

An independent set of linear seminvariants of $f_4$ is $a_0, a_1, a_2 + a_3$. The only linear invariant is $C_{020} = a_1 + a_2 + a_3$ $(= K,\ m = 4\ (§\,3))$. Multiplication of $K_1$ of $(5_1)$ and $C_{101}$ of § 1 by powers of $Q$ gives covariants of any odd order led by $a_1, a_0 + K$, and, by subtracting such covariants, covariants led by $a_0 + a_2 + a_3$.

Lemma. *There exists no covariant of odd order led by $K$.*

Assume such a covariant in the form $C = Kx_1^{2h+1} + Ix_1^{2h} x_2 + \cdots$. Then from (5), $m = 4$,

$$K(x_1^{2h+1} + x_1^{2h} x_2 t + \cdots) + I'(x_1^{2h} x_2 + \cdots) \equiv C \qquad (\mathrm{mod}\ 2),$$

where $I$ becomes $I'$ under (5). Hence, writing $I' \equiv I + tI_1$,

$$K \equiv I_1 \qquad (\mathrm{mod}\ 2).$$

Now if $I$ contains $a_4$, the increment $I_1$ contains $a_0$, whereas $K$ does not. Hence $I$ does not contain $a_4$. But the increment to a linear function of $a_0, a_1, a_2, a_3$ contains $a_1$ only, whereas $K$ contains $a_2$. Hence $K \not\equiv I_1$, a contradiction.

It now follows that the general form of a covariant of odd order is

$$C = [\lambda a_1 + \mu(a_0 + a_2 + a_3)]\, x_1^{2k+1} + \cdots.$$

Thus

$$C \equiv (\lambda + \mu) Q^k C_{101} + \mu Q^k K_1 + L\Gamma \qquad (\mathrm{mod}\ 2),$$

where $\Gamma$ is of even order $2k - 2$.

Any covariant of even order may be written

$$C_1 = [\lambda a_0 + \mu a_1 + \nu(a_2 + a_3)]\, x_1^{2h} + \cdots,$$

and we have, using $K_2$ $(m = 4)$ of § 3, and $C_{012}$ of § 1,

$$C_1 \equiv Q^{h-1}[\lambda K_2 + (\mu + \nu) C_{012}] + \nu K Q^h + L\Gamma_1 \qquad (\mathrm{mod}\ 2);$$

$\Gamma_1$ being a first degree covariant of odd order $2h - 3$. Hence the fundamental system sought is

$$K,\ K_1,\ K_2,\ C_{101},\ C_{012},\ L,\ Q. \tag{10}$$

The form $f_4$ itself is reducible as follows [cf. (8)]:

$$f_4 \equiv QK_2 + L(K_1 + C_{101}) \qquad (\mathrm{mod}\ 2).$$

Employing $K_1$, $K_2$, $K$, $K_{m3}$ $(m = 5)$ of § 3 and $C_{021}$, $C_{102}$ of § 1, we find for the required fundamental system of the quintic,

$$K,\ K_1,\ K_2,\ K_{53},\ C_{021},\ C_{102},\ L,\ Q. \tag{11}$$

The reduction of the form $f_5$ itself is given by

$$f_5 \equiv QK_{53} + L(K_2 + C_{102}) \qquad (\text{mod } 2) \qquad [\text{cf. } (9)].$$

## 6. On the complete system of the cubic, modulo 2

The development of the asyzygetic theory of the concomitants of a form often precedes the derivation of its complete system. In this section we show that every covariant of order $> 3$ of a binary cubic, modulo 2, is quasi-reducible (i. e., reducible on multiplication by $K^s$ $(s \geqq 0)$) in terms of a set of fourteen concomitants, nine covariants and five invariants.

It is known that the fundamental system of seminvariants* of $f_3$ modulo 2 is

$$\begin{gathered} a_0, \qquad K = a_1 + a_2, \qquad \delta_{00} = (a_0 + K + a_3)a_3, \\ \Delta = a_0 a_3 + a_1 a_2, \qquad \beta = a_1^2 + a_0 a_1, \end{gathered} \tag{12}$$

and also that $f_3$ has the invariants

$$\begin{gathered} K, \qquad \Delta, \qquad I = a_0^2 + a_0 K + \delta_{00}, \qquad k = a_0 \delta_{00}, \\ V = \beta(\beta + K^2 + a_0 K)(\Delta + \delta_{00}). \end{gathered} \tag{13}$$

In two previous papers (quoted above) I have shown that $f_3$ has the covariants†

$$\begin{aligned} H &= sx_1^2 + \Delta x_1 x_2 + (a_1 a_3 + a_2^2)x_2^2, \\ G_1 &= (\Delta + s)x_1 + (\Delta + a_1 a_3 + a_2^2)x_2 \qquad (s = a_0 a_2 + a_1^2), \\ P &= a_0^2 x_1^3 + a_1^2 x_1^2 x_2 + a_2^2 x_1 x_2^2 + a_3^2 x_2^3, \\ K_1 &= (a_0 + K)x_1 + (K + a_3)x_2, \\ K_2 &= a_0 x_1^2 + Kx_1 x_2 + a_3 x_2^2, \\ C_1 &= (a_0^2 + K^2)x_1 + (K^2 + a_3^2)x_2, \\ C_2 &= a_0^2 x_1^2 + K^2 x_1 x_2 + a_3^2 x_2^2. \end{aligned} \tag{14}$$

There is, therefore, a covariant led by $\beta$, viz.,

$$t = KK_2 + H = \beta x_1^2 + (\Delta + K^2)x_1 x_2 + (a_2 a_3 + a_2^2)x_2^2.$$

---

* Dickson, *Madison Colloquium Lectures*, p. 53.

† Cf. American Journal of Mathematics, loc. cit., p. 78. The forms $C_4^{(1)}$, $C_2^{(3)}$ in Table I are reducible as follows:

$$C_4^{(1)} \equiv LK_1 + QK_2, \qquad C_2^{(3)} \equiv Kt + (\Delta + K^2)K_2 \,(\text{mod } 2).$$

None of the invariants $\Delta$, $g$ (below), $I$ can be leading coefficients of covariants of odd order, but there exists a cubic covariant led by the invariant $K$, viz.,

$$G = QK_1 + f_3 = Kx_1^3 + (a_0 + a_1 + a_3)x_1^2 x_2 + (a_0 + a_2 + a_3)x_1 x_2^2 + Kx_2^3.$$

Taking the elementary symmetric function of second degree in the coefficients of $t$, as explained in § 3 (4), we have the fourth degree invariant of $f_3$,

$$(15) \quad g = \beta^2 + \beta(\Delta + K^2) + \beta\beta_1 + \beta_1(\Delta + K^2) + \beta_1^2 \qquad (\beta_1 = a_2 a_3 + a_2^2),$$
$$\equiv \beta^2 + \beta(\Delta + K^2) + (\Delta + \delta_{00})(\beta + a_0 K + K^2) \qquad (\text{mod } 2).$$

Now from (13), (15) we have

$$a_0^3 + a_0^2 K + a_0 I + k \equiv 0,$$

$$(16) \quad \begin{aligned} &\beta^2 + \beta(a_0^2 + a_0 K + I + K^2) \\ &\qquad + (a_0^2 + a_0 K + I + \Delta)(a_0 K + K^2) + g \equiv 0. \end{aligned}$$

Any seminvariant $\phi$ of $f_3$, being a polynomial in the seminvariants (12), is a polynomial in $a_0, K, \beta, \Delta, I$;

$$\phi = \phi(a_0, \beta, K, \Delta, I).$$

We now use congruences (16) as reducing moduli, whereupon we are able to reduce all exponents* of $\beta$ (in $\phi$) below 2 and all exponents of $a_0$ below 3. Thus any seminvariant can be reduced to the form

$$\phi = J_0 + J_1 a_0 + J_2 a_0^2 + (\Gamma_0 + \Gamma_1 a_0 + \Gamma_2 a_0^2)\beta,$$

wherein $J_i$, $\Gamma_i$ $(i = 0, 1, 2)$ are invariants (expressed in terms of $K, \Delta, k, I, g$) some of which might be zero. Let $C_M$ be any covariant of $f_3$ of even order $M = 2h$, led by $\phi$; $C_M = \phi x_1^{2h} + \cdots$. Then,

$$C_M \equiv Q^h J_0 + Q^{h-1}(K_2 J_1 + C_2 J_2)$$
$$+ Q^{h-1} t\Gamma_0 + Q^{h-2}(K_2 \Gamma_1 + C_2 \Gamma_2)t + LC \qquad (\text{mod } 2),$$

where $C$ is a covariant of odd order $2h - 3$. Thus every covariant of even order $> 3$ is reducible in terms of our covariants and invariants.

Proceeding to covariants of odd order; there is a covariant with seminvariant leader $B = \beta + \Delta$, viz.,

$$l = Bx_1^3 + (a_0 a_2 + a_1 a_2 + a_1 a_3 + a_2^2)x_1^2 x_2$$
$$+ (a_0 a_2 + a_1 a_2 + a_1 a_3 + a_1^2)x_1 x_2^2 + (\Delta + a_2 a_3 + a_2^2)x_2^3$$
$$\equiv QG_1 + Kf_3.$$

* Cf. L. J. Reed, *"Some fundamental systems of formal modular invariants and covariants,"* Dissertation, University of Pennsylvania, 1915, § 3.

Replacing $\beta$ by $B + \Delta$ in (16) and in $\phi$ we can reduce any seminvariant to the form

$$\phi = R_0 + R_1 a_0 + R_2 a_0^2 + (S_0 + S_1 a_0 + S_2 a_0^2) B,$$

where $R_i$, $S_i$ $(i = 0, 1, 2)$ are polynomials in the five invariants $K, \Delta, k, I, g$. Let $C_N$ be a covariant of $f_3$ of odd order $N = 2h + 3 > 3$, led by $\phi$; $C_N = \phi x_1^N + \cdots$. Then

$$\begin{aligned} KC_N \equiv Q^h R_0 G + KR_1 Q^h f_3 + KR_2 Q^h P \\ + K(lS_0 Q^h + lS_1 K_2 Q^{h-1} + lS_2 C_2 Q^{h-1}) + LC' \qquad (\text{mod } 2). \end{aligned}$$

We have now proved the following:*

THEOREM: *Every formal covariant modulo 2 of order $> 3$ of the binary cubic $f_3$ is quasi-reducible, upon multiplication by $K^s$ $(s \geqq 0)$, in terms of the fourteen concomitants listed below*:

$$K, \Delta, k, I, g, f_3, K_2, C_2, K_1, G_1, P, t, L, Q.$$

* *On the subject of quasi-reducibility in ternariant theory*, cf. Forsyth, American Journal of Mathematics, vol. 12 (1890).

UNIVERSITY OF PENNSYLVANIA