Now since B and C are Hermitian matrices each of the summations on the left is real. Hence, equating real and imaginary parts in (10) we have*

$$\alpha = \sum_{i,j} b_{ij}\bar{x}_i x_j,$$
$$\beta = \sum_{i,j} c_{ij}\bar{x}_i x_j.$$

If now we denote by η_i the absolute value of x_i and proceed as in (9), Corollaries 2 and 3 follow at once.

THE UNIVERSITY OF NORTH CAROLINA

ON THE REDUCTION OF THE INDEFINITE BINARY QUADRATIC FORMS†

BY J. V. USPENSKY

The reduction theory of the indefinite binary forms has been presented in widely different forms and from various points of view. But whatever point of view is adopted, it seems that Hermite's principle of continuous variables under more or less disguised form constitutes an essential foundation of all the existing theories of reduction.

Hermite's principle in its simplest aspect consists in association with a given indefinite form of a positive quadratic form containing a continuously varying positive parameter and the study of integral values of variables which give successive minima of the latter. However, the reduced forms in Hermite's theory differ from those in the classical Gaussian theory of reduction. A little contribution to the theory of reduction which this article contains has for its purpose to show how, by substituting for Hermite's positive quadratic form a certain nonhomogeneous function containing a variable positive parameter, we obtain precisely the Gaussian reduced forms.

Let

$$\xi = \alpha x + \beta y, \quad \eta = \gamma x + \delta y$$

* See Hirsch, loc. cit., p. 369.

† Presented to the Society, April 5, 1930.

be two independent linear forms. For the sake of simplicity we assume that the ratios $\alpha:\beta$ and $\gamma:\delta$ are irrational numbers so that neither of the forms ξ and η can vanish for integral values of the variables unless $x=y=0$. The function which takes the place of Hermite's positive form in the theory of reduction here developed is

$$F(x, y) = | \xi/\eta | + t | \eta |$$

where t is a continuously varying positive parameter. The variables x and y are supposed to be integers which do not vanish simultaneously. As $F(x, y)$ does not change if x and y are replaced by $-x$, $-y$ it is sufficient to consider such couples of integers (x, y) which make the second form η positive. It is almost evident that for a given positive value of $t=t_0$ there exists at least one couple of integers x, y giving a minimum value of $F(x, y)$. If such a couple is unique it will obviously be the only couple with such a property in a sufficiently small interval comprising the point $t=t_0$. If for $t=t_0$ there are several couples of integers giving the same minimum value of $F(x, y)$ we select one with the smallest η. This couple will give a minimum of $F(x, y)$ for $t=t_0$ and for all $t>t_0$ and sufficiently near to t_0. Thus there exist couples of integers which for certain values of the variable parameter are the only ones giving a minimum of $F(x, y)$. We shall call such couples of integers "minimizing couples." The whole question now is how to obtain all the minimizing couples.

Let (p_0, q_0) be one of the minimizing couples and τ the corresponding parameter value so that for $t=\tau$ the only system of integers giving a minimum of $F(x, y)$ is $x=p_0, y=q_0$ (provided the condition $\eta>0$ is satisfied). When t starts to decrease from τ the same couple which in a certain small neighborhood of τ continues to keep its property of being a minimizing couple cannot remain such in the whole interval from 0 to τ. For, given two numbers, ϵ however small and m however large, it is possible to find two integers x and y so as to satisfy the inequalities

$$| \xi | < \epsilon, \quad \eta > m$$

and it follows that corresponding to these integers $F(x, y)$ can be made less than any preassigned number if t becomes small enough whereas the same expression for $x=p_0$, $y=q_0$ remains greater than a certain determined positive number however small t is. Hence, we can conclude the existence of a certain number $t_1<\tau$ possessing the property that for $\tau \geqq t > t_1$ the couple p_0, q_0 is a unique minimizing couple, while for $t<t_1$ the same couple loses its minimizing property.

This can happen only in the following way: that for $t=t_1$ there are two minimizing couples; viz., p_0, q_0 and p_1, q_1, the latter taking the place of the former when t, decreasing, passes through the value t_1. We shall call this couple (p_1, q_1) the right neighbor of (p_0, q_0). If t begins to increase from τ in a similar manner we can see that the couple (p_0, q_0) ceases to give a minimum of $F(x, y)$ as soon as t passes through a certain value $t_0>\tau$ and is replaced by another minimizing couple (p_{-1}, q_{-1}), its left neighbor.

So every minimizing couple possesses perfectly determined right and left neighbors, and all the existing minimizing couples can be arranged in a single chain:

$$\cdots, (p_{-2}, q_{-2}), (p_{-1}, q_{-1}), (p_0, q_0), (p_1, q_1), (p_2, q_2), \cdots$$

extending indefinitely in both directions. Of two consecutive couples in this series the following is the right neighbor of the preceding one and the latter is the left neighbor of the former. The chain of minimizing couples leads to a chain of linear substitutions

$$\begin{pmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{pmatrix}; \qquad (i = \cdots, -2, -1, 0, 1, 2, \cdots).$$

We shall prove now the important property of this chain; namely, that all its substitutions are unimodular; that is, they have determinants ± 1. Let (p, q) and (p', q') be two minimizing couples, the second being the right neighbor of the first. It is evident that they both consist of relatively prime numbers. Furthermore, setting

$$\lambda = \alpha p + \beta q, \quad \lambda' = \alpha p' + \beta q',$$
$$\mu = \gamma p + \delta q, \quad \mu' = \gamma p' + \delta q',$$

we have by the properties of neighboring couples

$$\mu' > \mu > 0; \quad \left|\frac{\lambda'}{\mu'}\right| < \left|\frac{\lambda}{\mu}\right|; \tag{1}$$

and for suitable t

$$\left|\frac{\lambda}{\mu}\right| + t|\mu| = \left|\frac{\lambda'}{\mu'}\right| + t|\mu'| = P; \tag{2}$$

while for every couple of integers (x, y) differing from (p, q) and (p', q'), we have

$$\left|\frac{\xi}{\eta}\right| + t|\eta| \geqq P. \tag{3}$$

By means of the linear substitution

$$x = pX + p'Y, \quad y = qX + q'Y,$$

the forms ξ and η become

$$\xi = \lambda X + \lambda' Y, \quad \eta = \mu X + \mu' Y.$$

If the determinant has the value

$$pq' - p'q = \pm e, \ e > 1,$$

x and y will be integers if and only if we attribute to X, Y values of the form

$$X = \frac{a}{e}, \quad Y = \frac{b}{e}, \tag{4}$$

where a and b are integers satisfying the congruence

$$a + \mu b \equiv 0 \pmod{e}, \tag{5}$$

where μ is an integer determined by (p, q) and (p', q') and satisfying the conditions

$$0 < \mu \leqq e - 1.$$

If we substitute for X and Y their expressions (4), eliminate t by means of (2) and introduce the notations

$$\frac{\mu}{\mu'} = \sigma, \quad \frac{\lambda'}{\lambda} = \rho, \quad \rho\sigma = \epsilon,$$

the condition (3) can be presented as follows:

$$\frac{(1 - \sigma)|a\sigma + b\epsilon|}{|a\sigma + b|} + e^{-1}(1 - |\epsilon|)|a\sigma + b| \geqq 1 - \sigma|\epsilon|; \tag{6}$$

while instead of (1) we have

$$0 < \sigma < 1, \ |\epsilon| < 1.$$

The inequality (6) must be satisfied for every couple of integers satisfying (5). In particular, it must be satisfied if we take

$$a = e - \mu \leqq e - 1, \ b = 1.$$

Setting for brevity

$$a\sigma = \zeta, \qquad 0 < \zeta \leqq (e-1)\sigma,$$

we must have

$$(7)\ (1-\sigma)|\zeta+\epsilon| + e^{-1}(1-|\epsilon|)(\zeta+1)^2 \geqq (\zeta+1)(1-\sigma|\epsilon|).$$

But

$$(1-\sigma)|\zeta+\epsilon| + e^{-1}(1-|\epsilon|)(\zeta+1)^2$$
$$\leqq (1-\sigma)(\zeta+|\epsilon|) + e^{-1}(1-|\epsilon|)(\zeta+1),$$

and

$$(1-\sigma)(\zeta+|\epsilon|) + e^{-1}(1-|\epsilon|)(\zeta+1)^2 - (1-\sigma|\epsilon|)(\zeta+1)$$
$$= [1+\sigma\zeta - e^{-1}(\zeta+1)^2][|\epsilon|-1] < 0,$$

because in the interval $0 \leqq \zeta \leqq \sigma(e-1)$ the quadratic function

$$1+\sigma\zeta - e^{-1}(\zeta+1)^2$$

remains positive provided $e>1$. But the result obtained obviously contradicts (7), and hence $e=1$. Instead of (6) we now have

$$(8)\ (1-\sigma)|a\sigma+\epsilon b| + (1-|\epsilon|)(a\sigma+b)^2 \geqq (1-\sigma|\epsilon|)|a\sigma+b|,$$

and this must hold for *every* couple of integers a and b. By taking $a=1, b=1$, and $a=1, b=-1$ we obtain two conditions

$$(9) \qquad (1-\sigma)|\sigma+\epsilon| + (\sigma+1)(\sigma-|\epsilon|) \geqq 0,$$

$$(10) \qquad |\sigma-\epsilon| + 2\sigma|\epsilon| - \sigma - |\epsilon| \geqq 0.$$

We can show now that the inequality $\sigma < |\epsilon|$ is impossible. For, if $\epsilon>0$, we have

$$|\sigma-\epsilon| + 2\sigma|\epsilon| - \sigma - |\epsilon| = 2\sigma(\epsilon-1) < 0,$$

contrary to (10); and if $\epsilon<0$ we have

$$(1-\sigma)|\sigma+\epsilon| + (\sigma+1)(\sigma-|\epsilon|) = 2\sigma(\sigma+\epsilon) < 0,$$

contrary to (9). Thus necessarily $|\epsilon|<\sigma$, the equality being impossible as we suppose the ratio $\beta:\alpha$ to represent an irrational number. Now, if $\epsilon>0$, we have

$$|\sigma-\epsilon|+2\sigma|\epsilon|-\sigma-|\epsilon| = 2\epsilon(\sigma-1)<0,$$

which again contradicts (10) and therefore $\epsilon<0$, $-\epsilon<\sigma$; that is

$$(11) \qquad -1<\rho<0, \quad 0<\sigma<1.$$

Thus we reach the following conclusion. If (p, q) is a minimizing couple and (p', q') its right neighbor, then

$$pq'-p'q=\pm 1,$$

and

$$-1<\rho<0, \quad 0<\sigma<1.$$

It can be shown conversely that, if these conditions are fulfilled, (p, q) and (p', q') are both minimizing couples and (p', q') right neighbor of (p, q). To this end, it suffices to show that the inequality (8) holds *with the excluded sign of equality* for every couple of integers (a, b) different from $(\pm 1, 0)$ and $(0, \pm 1)$. Now that we know the sign of $\epsilon=\sigma\rho$, we can write this inequality as follows:

$$(12) \quad (\sigma-\sigma^2)|a+b\rho|+(1+\rho\sigma)(a\sigma+b)^2 \\ -(1+\rho\sigma^2)|a\sigma+b| \geqq 0.$$

Suppose at first that $a+b\rho<0$, which necesitates $b>a$, if we suppose $a>0$, which is legitimate. In this case, the left member of (12) coincides with the linear function ρ

$$P(\rho) = -(\sigma-\sigma^2)(a+b\rho)+(1+\rho\sigma)(a\sigma+b)^2 \\ -(1+\rho\sigma^2)(a\sigma+b),$$

and for extreme values of ρ:

$$\rho=-1 \quad \text{and} \quad \rho=-ab^{-1},$$

we have

$$P(-1) = (1-\sigma)[(a^2-a)\sigma^2+2a(b-1)\sigma+b^2-b] \geqq 0,$$

$$P(-ab^{-1}) = b^{-1}(b+\sigma a)[b^2-b-\sigma^2(a^2-a)]>0,$$

so that $P(\rho)>0$. Suppose now $a+b\rho>0$ and $a\sigma+b<0$, which necessitates $b<0$. In this case the left hand member of (12) coincides with the linear function of ρ

$$P(\rho) = (\sigma - \sigma^2)(a + b\rho) + (1 + \rho\sigma)(a\sigma + b)^2 + (1 + \rho\sigma^2)(a\sigma + b).$$

Now for $\rho = 0$ and $\rho = -1$, we have

$$P(0) = a(\sigma - \sigma^2) + (a\sigma + b)^2 + a\sigma + b,$$
$$P(-1) = (1 - \sigma)[\sigma(a - b) + (a\sigma + b)^2 + (1 + \sigma)(a\sigma + b)].$$

Since

$$\sigma(a - b) + (a\sigma + b)^2 + (1 + \sigma)(a\sigma + b) \\ - [a(\sigma - \sigma^2) + (a\sigma + b)^2 + a\sigma + b] = 2a\sigma^2 > 0,$$

it suffices to consider $P(0)$. We have then

$$P(0) = (a^2 - a)\sigma^2 + 2a(b + 1)\sigma + b^2 + b.$$

The minimum of this function is attained for

$$\sigma_0 = -(b + 1)(a - 1)^{-1},$$

and is

$$-(b + 1)(a - 1)^{-1}(a + b).$$

If $\sigma_0 \leqq 1$, we have $a + b \geqq 0$, and this minimum is $\geqq 0$. But for $\sigma = 0$ and $\sigma = 1$, we have

$$P(0) = b^2 + b \geqq 0, \quad P(0) = (a + b)^2 + (a + b) \geqq 0.$$

Therefore, for $0 < \sigma < 1$, we have $P(0) \geqq 0$, $P(-1) > 0$; and hence

$$P(\rho) > 0.$$

Next, if $a\sigma + b > 0$, the left member of (12) coincides with

$$P(\rho) = (\sigma - \sigma^2)(a + b\rho) + (1 + \rho\sigma)(a\sigma + b)^2 - (1 + \rho\sigma^2)(a\sigma + b)$$

Again

$$P(0) = a(\sigma - \sigma^2) + (a\sigma + b)^2 - (a\sigma + b),$$
$$P(-1) = (1 - \sigma)[\sigma(a - b) + (a\sigma + b)^2 - (1 + \sigma)(a\sigma + b)],$$

and

$$\sigma(a - b) + (a\sigma + b)^2 - (1 + \sigma)(a\sigma + b) \\ - [a(\sigma - \sigma^2) + (a\sigma + b)^2 - (a\sigma + b)] = -2b\sigma;$$

and this is >0 or <0 according as $b < 0$ or $b > 0$. If $b < 0$, we consider

$$P(0) = (a^2 - a)\sigma^2 + 2ab\sigma + b^2 - b.$$

For $\sigma=0$ and $\sigma=1$, this function assumes the values

$$b^2 - b > 0, \quad (a+b)^2 - (a+b) \geqq 0.$$

Its minimum is attained for

$$\sigma_0 = - b(a-1)^{-1},$$

and is

$$- b(a-1)^{-1}(a+b-1).$$

Now if $\sigma_0 \leqq 1$, we have

$$a+b-1 \geqq 0,$$

so that the minimum is $\geqq 0$. Therefore $P(0)\geqq 0$, if $0<\sigma<1$, and $P(-1)>0$; whence again

$$P(\rho) > 0.$$

Finally, if $b>0$, we consider the quadratic function

$$\sigma(a-b) + (a\sigma+b)^2 - (1+\sigma)(a\sigma+b)$$
$$= (a^2-a)\sigma^2 + 2b(a-1)\sigma + b^2 - b \geqq 0,$$

so that $P(-1)\geqq 0$ and $P(0)>0$, if $0<\sigma<1$. Hence $P(\rho)>0$. Thus the inequality (12) holds with the sign $>$ for every couple of integers (a, b) different from $(\pm 1, 0)$ and $(0, \pm 1)$; and this completes the proof of the statement.

Summing up, we can say that the conditions

$$pq' - p'q = \pm 1, \quad 0 < \sigma < 1, \quad -1 < \rho < 0,$$

are necessary and sufficient conditions in order that couples (p, q) and (p', q') should be two consecutive minimizing couples, the second being the right neighbor of the first. If we disregard the condition $\eta>0$, but instead suppose that the determinants of the substitutions in the chain belonging to the forms (ξ, η) have the value 1, then the preceding conditions are

$$pq' - p'q = 1, \quad |\sigma| < 1, \quad |\rho| < 1,$$

and σ and ρ have opposite signs.

After these preliminary investigations the reduction theory of the indefinite binary quadratic forms can be summarized in a few words.

Let

$$\phi = ax^2 + 2bxy + cy^2$$

be an indefinite form whose determinant $\mathfrak{D} > 0$ is not a perfect square. Denoting by

$$\omega = \frac{-b + \sqrt{\mathfrak{D}}}{a}, \qquad \omega' = \frac{-b - \sqrt{\mathfrak{D}}}{a}$$

the first and the second roots of ϕ, we introduce the linear forms

$$\xi = x - \omega y, \quad \eta = x - \omega' y,$$

and can form the chain of substitutions belonging to (ξ, η) or simply to ϕ. We call ϕ a *reduced form* if its chain contains the identical substitution

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Necessary and sufficient conditions for this are that we should have $|\omega| < 1$, $|\omega'| > 1$, and that ω and ω' of opposite signs. In this characteristic we recognize the Gaussian reduced forms. Every form Φ is equivalent to a reduced form. For if

$$\begin{pmatrix} p & p' \\ q & q' \end{pmatrix}$$

is a substitution belonging to the chain of Φ and we apply this substitution to Φ we obtain a form ϕ whose chain contains the identical substitution and therefore ϕ is a reduced form.

Finally, the fundamental proposition that two forms Φ and Φ' cannot be equivalent unless they have the same chain of reduced forms is almost intuitive from the adopted point of view. However, the same is true of every reduction theory based on Hermite's principle of continuous variables.

STANFORD UNIVERSITY