PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 3, March 1999, Pages 657–663
S 0002-9939(99)04535-9

THE DEDEKIND–MERTENS FORMULA AND DETERMINANTAL RINGS

WINFRIED BRUNS AND ANNA GUERRIERI

(Communicated by Wolmer V. Vasconcelos)

Abstract. We give a combinatorial proof of the Dedekind–Mertens formula by computing the initial ideal of the content ideal of the product of two generic polynomials. As a side effect we obtain a complete classification of the rank 1 Cohen–Macaulay modules over the determinantal rings $K[X]/I_2(X)$.

Let f, g be polynomials in one indeterminate over a commutative ring A. The Dedekind-Mertens formula relates the content ideals of f, g, and their product fg: one has

$$c(fg)c(f)^d = c(g)c(f)^{d+1}, \qquad d = \deg g.$$

It is the best universally valid variant of Gauß' classical formula $c(fg) = c(f)c(g)$ for polynomials over a principal ideal domain. (The content ideal of $f \in A[T]$ is the ideal generated by the coefficients of f in A.) Content ideals and the Dedekind–Mertens formula have recently received much attention; see Glaz and Vasconcelos [8], Corso, Vasconcelos, and Villarreal [6] and Heinzer and Huneke [9], [10]. For detailed historical information about the Dedekind–Mertens formula, see [9].

The main objective of this paper is a combinatorial proof of the formula based on a Gröbner basis approach to the ideal $c(fg)$ for polynomials with indeterminate coefficients; in fact we will determine the initial ideal of $c(fg)$ with respect to a suitable term order. (For information on term orders and Gröbner bases we refer the reader to Eisenbud [7].) A side effect of our approach is very precise numerical information about the rank one Cohen–Macaulay modules over the determinantal ring $S = K[X]/I_2(X)$ where X is an $m \times n$ matrix of indeterminates and $I_2(X)$ the ideal generated by its 2-minors. This connection extends the ideas of [6] and was in fact suggested by them. The actual motive for our work was the need for some explicit computation modulo $c(fg)$ in Boffi, Bruns, and Guerrieri [2], or, more precisely, modulo an ideal generalizing $c(fg)$ slightly.

Theorem 1. *Let K be a field, $R = K[Y_1, \dots, Y_m, Z_1, \dots, Z_n]$ and set*

$$d_k = \sum_{i+j=k} u_{ij} Y_i Z_j, \qquad k = 2, \dots, m+n,$$

Received by the editors January 22, 1997 and, in revised form, June 16, 1997.
1991 *Mathematics Subject Classification.* Primary 13C40, 13C14, 13D40, 13P10.
Key words and phrases. Dedekind–Mertens formula, initial ideal, determinantal ring, Cohen–Macaulay module.
The visit of the first author to the University of L'Aquila that made this paper possible was supported by the Vigoni program of the DAAD and the CRUI.

with $u_{ij} \in K$, $u_{ij} \neq 0$ for all i and j. Furthermore let $\mathcal{S}$ denote the set of the monomials

$$Y_{i_1} \cdots Y_{i_u} Z_{j_1} \cdots Z_{j_v}, \qquad 0 \le u < j_1,\ 0 \le v < m+1-i_u.$$

Then the set $\mathcal{N}$ of the monomials $\mu \notin \mathcal{S}$ generates the initial ideal of the ideal $I = (d_2, \dots, d_{m+n})R$ with respect to the reverse-lexicographic term order on R induced by the order

$$Y_1 > \cdots > Y_m > Z_1 > \cdots > Z_n$$

of the indeterminates. In particular, $\mathcal{S}$ is mapped to a K-basis of R/I under the natural homomorphism.

Proof. We first show that $\mathcal{N}$ is contained in the initial ideal $\operatorname{in}(I)$. Each $\mu \in \mathcal{N}$ is divisible by one of the monomials (1) $Y_i Z_{j_1} \cdots Z_{j_v}$ with $i \ge m+1-v$ or (2) $Y_{i_1} \cdots Y_{i_u} Z_j$ with $j \le u$. Therefore it is enough to consider the monomials of type (1) and type (2).

(1) In order to conclude that $\mu = Y_i Z_{j_1} \cdots Z_{j_v} \in \operatorname{in}(I)$ we show the following claim: modulo I the monomial μ is a K-linear combination of monomials $Y_k \nu$ where ν is a monomial in $Z_1, \dots, Z_n$ with $\nu < Z_{j_1} \cdots Z_{j_v}$ and $k < m+1-v$. (Of course, we allow the linear combination to be empty, in which case $\mu \in I$.) In fact, μ is the initial monomial of the element of I representing the relation between μ and the $Y_k \nu$ modulo I.

The claim is proved by induction on v. In the case $v = 1$ one simply uses that $Y_m Z_{j_1}$ is the initial monomial of d_{m+j_1} and that the other monomials occurring in d_{m+j_1} satisfy the requirements of the claim.

In the case $v > 1$ we must use an additional induction on $Z_{j_1} \cdots Z_{j_v}$ with respect to the term order. In the first step we replace $Y_i Z_{j_1}$ by a linear combination of the other monomials $Y_r Z_s$ in d_{i+j_1}. If $s > j_1$, then $Z_s Z_{j_2} \cdots Z_{j_v} < Z_{j_1} \cdots Z_{j_v}$ in the term order; if in addition $r < m+1-v$, then $Y_r Z_s Z_{j_2} \cdots Z_{j_v}$ is compatible with our claim, and otherwise we may use induction on the term order.

Suppose now that $s < j_1$. Then $r \ge m+1-(v-1)$, and we can apply induction on v to $Y_r Z_{j_2} \cdots Z_{j_v}$. Thus we can replace $Y_r Z_{j_2} \cdots Z_{j_v}$ by a linear combination of monomials $Y_q Z_{k_2} \cdots Z_{k_v}$ with $Z_{k_2} \cdots Z_{k_v} < Z_{j_2} \cdots Z_{j_v}$. (We need not take care of q). Now it only remains to check whether $Z_s Z_{k_2} \cdots Z_{k_v} < Z_{j_1} \cdots Z_{j_v}$; if so, we can again apply induction on the term order.

We rewrite $Z_s Z_{k_2} \cdots Z_{k_v} = Z_{l_1} \cdots Z_{l_v}$ with $l_1 \le \cdots \le l_v$. Whether $s \le k_2$ or otherwise, one has

$$Z_{l_2} \cdots Z_{l_v} \le Z_{k_2} \cdots Z_{k_v} < Z_{j_2} \cdots Z_{j_v}.$$

This implies $Z_{l_1} \cdots Z_{l_v} < Z_{j_1} \cdots Z_{j_v}$ since $j_1 \le j_2$. (It is of course essential that we are using the reverse-lexicographic term order in which $Z_1 > \cdots > Z_m$.)

(2) We claim: modulo I a monomial $\mu = Y_{i_1} \cdots Y_{i_u} Z_j$ with $j \le u$ is a K-linear combination of monomials νZ_k with $k > u$ and a monomial ν in $Y_1, \dots, Y_m$. Observe that no condition on ν is necessary: $k > j$ implies that $\nu Z_k < \mu$; thus μ is the initial monomial of the element of I representing the relation established by the claim.

The substitution $Y_i \mapsto Y_{m+1-i}$, $Z_j \mapsto Z_{n+1-j}$ induces an automorphism on R that maps the ideal I onto itself. Therefore we can replace our claim by the following: modulo I a monomial $Y_{i_1} \cdots Y_{i_u} Z_j$ with $j \ge n+1-u$ is a K-linear combination of monomials νZ_k with $k < n+1-u$ and a monomial ν in $Y_1, \dots , Y_m$. However, this has been proved in (1) with the roles of Y and Z exchanged.

It remains to show that the monomials in $\mathcal{S}$ are linearly independent modulo I. To this end we introduce the subalgebra

$$S = K[Y_iZ_j \colon i = 1, \dots , m,\ j = 1, \dots , n].$$

The elements d_k belong to S, and we set $J = (d_2, \dots , d_{m+n})S$. As an S-module, R decomposes into the direct sum

$$R = \bigoplus_{\delta\in\mathbb{Z}} M_\delta,$$

where M_δ is the K-vector space generated by all monomials μ such that $\deg_Y \mu - \deg_Z \mu = \delta$ ($\deg_Y \mu$ is the number of factors Y_i dividing μ). Then $M_0 = S$. As an S-module, M_δ, $\delta \geq 0$, is generated by the monomials $Y_{i_1} \cdots Y_{i_\delta}$, and a corresponding statement holds for M_δ, $\delta \leq 0$, and the monomials $Z_{j_1} \cdots Z_{j_{-\delta}}$.

This decomposition of R induces the decomposition $R/I \cong \bigoplus_{\delta\in\mathbb{Z}} M_\delta/JM_\delta$ of S/J-modules. Since each monomial in $\mathcal{S}$ belongs to one of the direct summands, it is enough to prove the linear independence of the monomials in $\mathcal{S} \cap M_\delta$ modulo JM_δ. We have already shown that their residue classes span M_δ/JM_δ as a vector space.

Suppose first that $\delta \geq n-1$ or $\delta \leq -(m-1)$. Then the elements of $\mathcal{S} \cap M_\delta$ are the monomials

$$Y_{i_1} \cdots Y_{i_\delta} \qquad \text{and} \qquad Z_{j_1} \cdots Z_{j_{-\delta}},$$

respectively. It is obvious that they are linearly independent modulo JM_δ.

In the cases $-(m-1) \leq \delta \leq n-1$ we count the elements of $\mathcal{S} \cap M_\delta$. (The values $\delta = n-1$ and $\delta = -(m-1)$ in which both arguments overlap are of special interest.) Suppose first that $\delta \geq 0$. Then $\mathcal{S} \cap M_\delta$ consists exactly of the monomials

$$Y_{i_1} \cdots Y_{i_u} Z_{j_1} \cdots Z_{j_{u-\delta}}, \qquad i_u \leq m-u+\delta,\ j_1 \geq u+1,$$

where u ranges over all positive integers $\geq \delta$. However, the inequalities can only be satisfied by at least one monomial if $u \leq m+\delta-1$ and $u \leq n-1$. With $N = \min(m+\delta-1, n-1)$, we have

$$\begin{aligned}\dim_K M_\delta/JM_\delta \leq \#(\mathcal{S} \cap M_\delta) &= \sum_{u=\delta}^{N} \binom{(m-u+\delta)+u-1}{u}\binom{(n-u)+u-\delta-1}{u-\delta}\\ &= \sum_{v=0}^{N-\delta} \binom{(m-1)+\delta}{m-1-v}\binom{(n-1)-\delta}{v}\\ &= \binom{(m-1)+(n-1)}{m-1}.\end{aligned}$$

For $-(m-1) \leq \delta \leq 0$ one obtains the same result.

But we also have a lower bound on $\dim_K M_\delta/JM_\delta$. Note that M_δ is a rank 1 module over S: multiplication by Z_1^δ in the case $\delta \geq 0$ and $Y_1^{(-\delta)}$ in the case $\delta \leq 0$ maps M_δ bijectively onto a non-zero ideal of S. It is well known that

$$S \cong K[X]/I_2(X),$$

where X is an $m \times n$ matrix of indeterminates, $I_2(X)$ the ideal generated by its 2-minors, and the isomorphism is induced by the substitution $X_{ij} \mapsto Y_iZ_j$. The

1-forms d_k form a system of parameters in S. This follows as in the special case in which $u_{ij} = 1$ for all i and j (for example, see Bruns and Vetter [4], (5.9)). Therefore

$$\dim_K M_\delta / JM_\delta \geq e(S),$$

where $e(S)$ is the multiplicity of S; see Bruns and Herzog [3], 4.6.11. The multiplicity of S is

$$e(S) = \binom{(m-1)+(n-1)}{m-1};$$

it is not hard to compute since S is the Segre product of the polynomial rings $K[Y_1, \dots, Y_m]$ and $K[Z_1, \dots, Z_n]$ (see Herzog and Trung [11] for the multiplicities of determinantal rings in general).

Since $\#(\mathcal{S} \cap M_\delta) \leq \dim_K M_\delta / JM_\delta$ and $\mathcal{S} \cap M_\delta$ represents a system of generators of M_δ / JM_δ, we conclude that $\mathcal{S} \cap M_\delta$ represents a basis of M_δ / JM_δ and that

$$\dim_K M_\delta / JM_\delta = \binom{(m-1)+(n-1)}{m-1} = e(S).$$

In conjunction with the linear independence of $\mathcal{S}$ modulo I, the inclusion $\mathcal{N} \subset \operatorname{in}(I)$ implies that $\operatorname{in}(I)$ is generated by $\mathcal{N}$. □

Our first corollary is the Dedekind–Mertens formula.

Corollary 2. *Let A be a commutative ring, $f, g \in A[T]$, and set $d = \deg g$. Then*

$$c(fg)c(f)^d = c(g)c(f)^{d+1}.$$

In general, the exponent d cannot be replaced by a smaller number.

Proof. It is enough to treat the "generic" case in which the coefficients of f and g are indeterminates over $\mathbb{Z}$, and A is the polynomial ring over $\mathbb{Z}$ in these indeterminates. Furthermore, the formula holds over $\mathbb{Z}$ if and only if it holds over $\mathbb{Q}$ and modulo all prime numbers p. Therefore we may then replace $\mathbb{Z}$ by a field.

Let $U_0, \dots, U_c$ and $V_0, \dots, V_d$ be the coefficients of f and g, respectively. Then $c(fg)$ is generated by the elements $\sum_{i+j=k} Y_i Z_j$, and we are in the situation of the theorem upon setting $m = c+1$, $n = d+1$, $Y_i = U_{i+1}$, and $Z_j = V_{j+1}$.

The inclusion "$\subset$" holds for trivial reasons, and to verify the converse we must show that every monomial μ with $\deg_Y \mu = d+1$ and $\deg_Z \mu = 1$ is contained in I (with the notation of the theorem). However, the standard basis $\mathcal{S}$ contains no monomial of bidegree $(n, 1)$ and J is generated by bihomogeneous elements. Therefore all monomials of bidegree $(n, 1)$ belong to I.

Since $\mathcal{S}$ contains monomials of bidegree $(n-1, 1)$, the exponent d cannot be reduced. (In [6] this was proved in the case in which $\deg g \leq \deg f$; the argument uses information on the Hilbert series of S that, for example, is contained in Corollary 4 below.) □

The proof of the theorem has given us very precise information on the modules M_δ. This information can be interpreted homologically.

Corollary 3. *With the notation introduced in the proof of the theorem, the modules M_δ, $-(m-1) \leq \delta \leq n-1$, represent the isomorphism classes of rank 1 Cohen–Macaulay S-modules.*

Proof. If $\delta \geq 0$, then multiplication by Z_1^δ maps M_δ isomorphically on the δ-th power of the ideal Q generated by the elements $x_{i1} = Y_i Z_1$ in S. An analogous statement holds for $\delta \leq 0$ and the ideal P generated by the x_{1j}. By a result of Bruns (see [4], (8.4) and (9.18)) the powers of P and Q represent the divisor classes of S. Therefore it only remains to find out which of the modules M_δ are Cohen–Macaulay.

Since $\operatorname{rank} M_\delta = 1$, its Cohen–Macaulay property is equivalent to the equation $\dim_K M_\delta / JM_\delta = e(S)$; see [3], 4.6.11. We have verified this equation for $-(m-1) \leq \delta \leq n-1$. For all other values of δ, the minimal number of generators of M_δ exceeds $e(S)$. □

The Cohen–Macaulay property of M_{n-1} is actually equivalent to the Dedekind–Mertens formula. In fact, let $\mathfrak{m}$ be the irrelevant maximal ideal of S. Then $\dim_K M_{n-1}/\mathfrak{m}M_{n-1} = e(S)$ so that the equality $\dim_K M_{n-1}/JM_{n-1} = e(S)$ forces JM_{n-1} to be equal to $\mathfrak{m}M_{n-1}$. This is another way to read the Dedekind–Mertens formula.

It seems that the exact value of $\operatorname{depth} M_\delta$ is not known for δ outside the range specified in the lemma. However, its asymptotic values have been computed: $\operatorname{depth} M_\delta = n-1$ for $\delta \gg 0$ and $\operatorname{depth} M_\delta = m-1$ for $\delta \ll 0$ (see [4], (9.27)(c)).

It would be interesting to generalize Corollary 3 to all the determinantal rings $S_r = K[X]/I_{r+1}(X)$. The divisor classes of S_r are again represented by the powers of the ideal P generated by the r-minors of the first r rows and the powers of the corresponding ideals for the columns. An easy localization argument (ubiquitous in [4]) by which the Cohen–Macaulay property descends to the case $r = 1$ shows that P^k and Q^l can only be Cohen–Macaulay for $k \leq m-r$ and $l \leq n-r$, and we conjecture that they are indeed Cohen–Macaulay for these values.

For the previous corollary only the multiplicity of M_δ was used, but we have actually computed its Hilbert series. The Hilbert series can be written as a rational function

$$H(t) = \frac{h_0 + h_1 t + \cdots + h_s t^s}{(1-t)^{m+n-1}},$$

since $\dim_K M_\delta = \dim_K S = m+n-1$. In the next corollary we confine ourselves to the case $\delta \geq 0$. The other case follows by exchanging m and n, δ and $-\delta$.

Corollary 4. *The coefficients of the numerator of the Hilbert series of M_δ, $\delta \geq 0$, are given by*

$$h_u = \begin{cases} \binom{m-1+\delta}{u}\binom{n-1-\delta}{u-\delta} & \delta \leq u \leq \min(m-1+\delta, n-1), \\ 0 & \textit{else}. \end{cases}$$

Proof. Since M_δ is Cohen–Macaulay, the homogeneous system of parameters $d_1, \dots, d_{m+n}$ is a regular sequence on M_δ. Therefore $h_u = \dim_K (M_\delta/JM_\delta)_u$, where the index u indicates the graded component of degree δ. (The elements $x_{ij} = Y_i Z_j$ have degree 1 in S.) This number has been computed in the proof of the theorem. □

It is not hard to check that among all the modules M_δ exactly one has the highest coefficient $h_s = 1$, namely M_{n-m}. It follows immediately that M_{n-m} is the canonical module of S, a result that has been shown by another approach in [4]. For $\delta = 0$, $M_\delta = S$, one can also compute the Hilbert series using the fact that S is the Segre product of the polynomial rings $K[Y_1,\dots,Y_m]$ and $K[Z_1,\dots,Z_n]$. (See Conca and Herzog [5] for the Hilbert series of determinantal rings in general).

Some further aspects of our results have been collected in the following remarks.

Remarks 5. (a) From the view point of determinantal rings, a basis of M_δ/JM_δ, $\delta\ge 0$, in terms of the generators $Y_{i_1}\cdots Y_{i_\delta}$ of M_δ and the generators x_{jk} of S may be more natural. By methods similar to those applied in the proof of the theorem one can show that the elements

$$Y_{i_1}\cdots Y_{i_\delta}x_{j_1k_1}\cdots x_{j_uk_u},\qquad i_1\le\cdots\le i_\delta<j_1\cdots<j_u<m,\ \delta+1<k_1<\dots k_u,$$

represent a K-basis of M_δ/JM_δ. (For $\delta\le 0$ one has a dual statement.) In particular, the defining ideal of S/J as a residue class ring of $K[X]$ has a Gröbner basis of degree 1 and 2 elements with respect to a suitable term order.

(b) Our results can be formulated for more general rings of coefficients than fields. For example, let A be a commutative ring and set $R=A[Y_1,\dots,Y_m,Z_1,\dots,Z_n]$. If the coefficients u_{ij} of $d_2,\dots,d_{m+n}$ are units in A, then R/I is a free A-module, and the set $\mathcal{S}$ represents a basis of R/I.

This is easily reduced to the case of a field of coefficients. In fact, it is enough to show the statement for the case in which $A=\mathbb{Z}[U_{ij}^{\pm 1}]$ is a Laurent polynomial ring over $\mathbb{Z}$. For R/I to be free with basis $\mathcal{S}$ over an integral domain A, it suffices that the dimension of $R/I\otimes Q(A)$ coincides with the cardinality of $\mathcal{S}$ where $Q(A)$ is the field of fractions of A. But this follows from Theorem 1 and its proof; in showing that $\mathcal{S}$ generates R/I we have only used that the u_{ij} are units.

(c) For an application in [2] we note that $\mu=Y_1^{n-1}Z_n^{m-1}$ belongs to $\mathcal{S}$, and is therefore non-zero modulo I. However, one has $Y_i\mu\in I$ and $Z_j\mu\in I$ for all i and j since $\mathcal{S}$ contains no element ν with $\deg_Y\nu\ge n$ or $\deg_Z\nu\ge m$.

We can say even more: μ is the only element of bidegree $(n-1,m-1)$ in $\mathcal{S}$; therefore it generates the bidegree $(n-1,m-1)$ component of R/I. The same is true for $\mu'=Y_m^{n-1}Z_1^{m-1}$ since the automorphism given in the proof of Theorem 1 maps μ to μ'. Therefore there exists $a\in K$, $a\ne 0$, with $\mu'\equiv a\mu$ modulo I. As the whole argument also works over $\mathbb{Z}$ (see (b)), one actually has $a=\pm 1$.

(d) The theorem was suggested by MACAULAY [1].

References

1. D. Bayer and M. Stillman. *Macaulay: a system for computation in algebraic geometry and commutative algebra.* Available by anonymous `ftp` from `zariski.harvard.edu`.
2. G. Boffi, W. Bruns, and A. Guerrieri. *On the jacobian ideal of a trilinear form.* Preprint.
3. W. Bruns and J. Herzog. *Cohen—Macaulay rings.* Cambridge University Press 1993. MR **95h:**13020
4. W. Bruns and U. Vetter. *Determinantal rings.* Lect. Notes Math. **1327**, Springer 1988. MR **89i:**13001
5. A. Conca and J. Herzog. *On the Hilbert function of determinantal rings and their canonical module.* Proc. Amer. Math. Soc. **122** (1994), 677–681. MR **95a:**13016
6. A. Corso, W. V. Vasconcelos, and R. Villareal. *Generic Gaussian Ideals.* J. Pure Appl. Algebra, to appear.
7. D. Eisenbud. *Commutative algebra with a view towards algebraic geometry.* Springer, 1995. MR **97a:**13001
8. S. Glaz and W. V. Vasconcelos. *The content of Gaussian polynomials.* J. Algebra, to appear
9. W. Heinzer and C. Huneke. *The Dedekind–Mertens Lemma and the contents of polynomials.* Proc. Amer. Math. Soc., to appear.

10. W. Heinzer and C. Huneke. *Gaussian polynomials and content ideals.* Proc. Amer. Math. Soc., to appear.
11. J. Herzog and N. V. Trung. *Gröbner bases and multiplicity of determinantal and pfaffian ideals.* Adv. in Math. **96** (1992), 1–37. MR **94a:**13012

Universität Osnabrück, FB Mathematik/Informatik, 49069 Osnabrück, Germany
E-mail address: Winfried.Bruns@mathematik.uni-osnabrueck.de

Università di L'Aquila, Dip. di Matematica, Via Vetoio, Coppito, 67010 L'Aquila, Italy
E-mail address: guerran@univaq.it