DIMACS Series in Discrete Mathematics
and Theoretical Computer Science

Patterns of Dependence among Powers of Polynomials

Bruce Reznick

ABSTRACT. Let $F = \{f_1, \dots, f_r\}$ be a family of polynomials and let the ticket of F, $T(F)$, denote the set of integers m so that $\{f_j^m\}$ is linearly dependent. We show that $|T(F)| \le \binom{r-1}{2}$ and present many concrete tickets. For example, let ζ denote a primitive fifth root of unity, and let $f_j(x,y) = \zeta^j x^2 + ixy + \zeta^{-j} y^2$, $0 \le j \le 4$. Then $T(\{f_0, \dots, f_4, xy\}) = \{1, 2, 3, 4, 8, 14\}$.

1. Introduction and definitions

The motivation for this paper is a remarkable example due to A. H. Desboves in 1880 (see [**3**, p.684]) and, independently, N. Elkies (see [**2**, p.542]) in 1995.

EXAMPLE 1. Let

$$
\begin{aligned}
f_1(x,y) &= x^2 + \sqrt{2}xy - y^2, \quad f_2(x,y) = ix^2 - \sqrt{2}xy + iy^2, \\
f_3(x,y) &= -x^2 + \sqrt{2}xy + y^2, \quad f_4(x,y) = -ix^2 - \sqrt{2}xy - iy^2.
\end{aligned}
\tag{1.1}
$$

Then $\sum_j f_j^5 = 0$. It is not hard to show that $\sum_j f_j = \sum_j f_j^2 = 0$ as well; however, $\{f_j^m\}$ is linearly independent for other integers m. This is surprising, and not only because of the gap in the exponents. Let $M_m(t_1, t_2, t_3, t_4) = \sum_j t_j^m$. Then (f_1, f_2, f_3, f_4) lies in the intersection $\{M_1 = 0\} \cap \{M_2 = 0\} \cap \{M_5 = 0\} \subset \mathbb{C}^4$. This is not what one would expect geometrically. However, Newton's Theorem for symmetric forms implies that M_5 is in the ideal (M_1, M_2), so $\{M_5 = 0\}$ is contained in $\{M_1 = 0\} \cap \{M_2 = 0\}$. We shall return to this example throughout the paper from varying points of view, and prove the assertions of this paragraph.

Let $F = \{f_j\}$ be a finite set of polynomials. The *ticket* of F, $T(F)$, is defined by

$$T(F) = \{m \in \mathbb{N} : \{f_j^m\} \text{ is linearly dependent}\}.$$

EXAMPLE 2. Here are some families with tickets that are easy to verify by hand.

$$
\begin{aligned}
T(\{x,y,z\}) &= \emptyset, \\
T(\{x,y,x+y\}) &= \{1\}, \\
T(\{x^2-y^2, 2xy, x^2+y^2\}) &= \{2\}.
\end{aligned}
\tag{1.2}
$$

1991 *Mathematics Subject Classification.* Primary 11D41, 11E76, 14Q15, 32H25; Secondary 11P05, 15A99, 30D35.

We let $\overline{m}(F)$ denote the maximum element of $T(F)$, with the understanding that $\overline{m}(F) = 0$ if $T(F) = \emptyset$. More specifically, for integers $r \geq 2$, $n \geq 2$, $d \geq 1$, let $\mathcal{F}(r,n,d)$ denote the set of families $F = \{f_1, \dots, f_r\}$, where each f_j is a homogeneous polynomial over $\mathbb{C}$ in n variables of degree d, and no two f_j's are proportional. Let

$$\mathcal{T}(r,n,d) = \{T(F) : F \in \mathcal{F}(r,n,d)\}.$$

Let $\overline{m}_r$ denote the maximum of $\overline{m}(F)$, given $|F| = r$. It is known that $\overline{m}_r \leq r^2 - 2r$. We shall say that $F \in \mathcal{F}(r,n,d)$ is a *dysfunctional* family if $|T(F)| > r-2$. (The term "dysfunctional" refers to excessive dependence, as in Example 1.)

One of the principal goals of this research is to determine $\mathcal{T}(r,n,d)$. We are able to do so in the cases $r \leq 3$, $(n,d) = (2,1)$, and $(r,n,d) = (4,2,2)$.

It is not difficult to show that any finite set of integers can appear as a ticket. Indeed, let ζ denote a primitive d-th root of unity, and let

$$F_d^* := \{x^d + y^d, x^d + \zeta y^d, x^{d-1}y, \dots, xy^{d-1}\} \in \mathcal{F}(d+1,2,d).$$

We show in Example 13 that $T(F_d^*) = \{d\}$. Now suppose that $A = \{m_j\}$ is given and consider $F = \cup F_{m_j}^*$, where each form in $F_{m_j}^*$ is binary in the variables (x_j, y_j). It is then easy to see that $T(F) = A$. More generally, if $T(F_1) = T_1$ and $T(F_2) = T_2$, and if F_1 and F_2 involve disjoint sets of variables, then $T(F_1 \cup F_2) = T_1 \cup T_2$. Since this seems like cheating, we shall say that a family F is *indecomposable* if there does not exist a nontrivial partition $F = F_1 \cup F_2$ so that $T(F) = T(F_1) \cup T(F_2)$.

CONJECTURE 1.1. Every finite subset of $\mathbb{N}$ appears as the ticket of some indecomposable family.

There does not seem to be much in the literature on tickets, *per se*, except for some discussion of $\overline{m}_r$.

If $r = 3$, then after scaling, $m \in T(F)$ implies that $f_1^m + f_2^m - f_3^m = 0$. In 1879, J. Liouville proved (see [**14**, p.263]) that Fermat's Last Theorem is true for non-constant polynomials; considering (1), we see that $\overline{m}_3 = 2$.

J. Molluzzo, in his 1972 thesis [**10**] (cited in [**11**]) shows that $\overline{m}_r \geq \lfloor r^2/4 \rfloor - 1$. We shall discuss Molluzzo's construction in Example 12. The bound for $\overline{m}_r$ is slightly improved in Example 9 for $r \leq 6$.

M. Green proved in 1975 [**4**, p.71] that if $\{\phi_j\}$, $1 \leq j \leq r$, are holomorphic functions in n complex variables, no two of which are proportional, and $\sum_{j=1}^r \phi_j^m = 0$, then $m \leq (r-1)^2 - 1$. This implies that $\overline{m}_r \leq r(r-2)$.

D. J. Newman and M. Slater [**11**] discussed Waring's Problem for polynomials; upon homogenizing their polynomials, one obtains information about $T(F)$ if one of the f_j's is the d-th power of a linear form. Their work was generalized by J. F. Voloch [**15**] to equations over function fields.

There is also a connection to Nevanlinna theory – see [**8**], [**9**]. If $m \in T(F)$ for $F \in \mathcal{F}(r,2,d)$, then by dehomogenizing and transposing the linear relation among f_j^m, we obtain an equation $\sum_{j=1}^{r-1} \phi_j^m(z) = 1$ in rational functions ϕ_j of a single complex variable. A very recent survey of this work is [**6**]. W. Hayman [**8**] proved in 1985 that if $\sum_{j=1}^3 \phi_j^m(z) = 1$ for rational functions ϕ_j, then $r \leq 7$; thus, $\overline{m}_4 \leq 7$. Example 1 shows that $\overline{m}_4 \geq 5$. G. Gundersen [**5**] has found meromorphic (not rational) functions g_j for which $g_1^6(z) + g_2^6(z) + g_3^6(z) = 1$.

We now collect some trivial remarks, which will be used without citation throughout the rest of the paper. If $f_j = \alpha f_i$, then f_i^m and f_j^m are dependent for every m, so $T(F)$ is uninteresting. This explains the non-proportionality condition in the definition of $\mathcal{F}(r,n,d)$.

The dimension of the vector space of forms of degree D in n variables is $\binom{n+D-1}{n-1}$. Thus, if $F \in \mathcal{F}(r,n,d)$ and if $r > \binom{n+md-1}{n-1}$, then $\{f_j^m\}$ must be dependent. In this case we say that m is *forced* to be in $T(F)$.

There is no *a priori* reason to assume that the polynomials in a given family F are all homogeneous and of the same degree, but this restriction is harmless. Suppose $F = \{f_j\}$, $1 \le j \le r$, where each f_j is a polynomial in n variables of degree $\le d$. Homogenize F by defining

$$f_j'(x_1,\dots,x_{n+1}) = x_{n+1}^d f_j\left(\frac{x_1}{x_{n+1}},\dots,\frac{x_n}{x_{n+1}}\right), \qquad 1 \le j \le r,$$

and let $F' = \{f_j'\} \in \mathcal{F}(r,n+1,d)$. It is easy to see that $T(F) = T(F')$. Similarly, if we dehomogenize $G = \{g_j\} \in \mathcal{F}(r,n,d)$, via

$$g_j'(x_1,\dots,x_{n-1}) = g_j(x_1,\dots,x_{n-1},1), \qquad 1 \le j \le r,$$

and let $G' = \{g_j'\}$, then $T(G) = T(G')$.

If $F = \{f_j\}$ and

$$f_j'(x_1,\dots,x_n) = f_j\left(\sum_{k=1}^n \alpha_{1k}x_k + \beta_1, \cdots \sum_{k=1}^n \alpha_{nk}x_k + \beta_n\right), \qquad 1 \le j \le r,$$

where $\det([\alpha_{jk}]) \ne 0$, and $F' = \{f_j'\}$, then clearly $T(F) = T(F')$: the ticket of a family is not changed by a simultaneous affine invertible linear change of variables.

As a special case of this, if $F = \{f_j\}$, $f_j' = \lambda_j f_j$, where $\lambda_j \ne 0$ and $F' = \{f_j'\}$, then $T(F) = T(F')$. That is, we may normalize the members of a family without affecting its ticket. In particular, if $\sum_j c_j f_j^m = 0$, $c_j \ne 0$, then we may assume without loss of generality that $c_j = \pm 1$ at our convenience. (Of course, we can only do this for *one* such exponent $m \in T(F)$.)

Given $\{f_j\}$ in n variables and n polynomials $\psi_k(y_1,\dots,y_m)$, we can define

$$f_j'(y_1,\dots,y_m) := f_j(\psi_1(y),\dots,\psi_n(y)).$$

Then $\sum_{j=1}^r \lambda_j f_j = 0$ implies $\sum_{j=1}^r \lambda_j f_j' = 0$. It is possible that the f_j''s might not be pairwise non-proportional, but it might also be possible that a judicious choice of ϕ_k will allow for the ticket to be extended. For example, $T(\{x+y, x-y\}) = \emptyset$ and $4xy = (x+y)^2 - (x-y)^2$ is not a square, but if we replace x and y by x^2 and y^2 and add $2xy$ to the family, we put 2 into the ticket; c.f. (1).

If $0 \ne g$ is a form, then $T(\{f_j\}) = T(\{gf_j\})$. Thus, $d < d'$ implies trivially that $\mathcal{T}(r,n,d) \subseteq \mathcal{T}(r,n,d')$.

If $n < n'$, then by viewing $f_j(x_1,\dots,x_n)$ as a form in $(x_1,\dots,x_n,x_{n+1},\dots,x_{n'})$, we see that $\mathcal{T}(r,n,d) \subseteq \mathcal{T}(r,n',d)$.

Regrettably, it is not true that $r < r'$ implies $\mathcal{T}(r,n,d) \subseteq \mathcal{T}(r',n,d)$. For example, $T(\{x,y\}) = \emptyset$, so $\emptyset \in \mathcal{T}(2,2,1)$. However, $m = 1$ is forced to be in $T(F)$ for every $F \in \mathcal{F}(3,2,1)$. We suspect that the only exceptions to the inclusion $\mathcal{T}(r,n,d) \subseteq \mathcal{T}(r',n,d)$ are consequences of such forcing.

Here is an outline of the rest of this paper. In section two, we prove our main theoretical result: if $F \in \mathcal{F}(r,n,d)$, then $|T(F)| \le \binom{r-1}{2}$. The proof gives an explicit non-zero polynomial in $(m,x_1,\dots,x_n)$ which vanishes identically when $m \in T(F)$. This is a modest improvement on the bound $|T(F)| \le r(r-2)$, which follows immediately from Green's bound on $\overline{m}_r$. In section three, we analyze $\mathcal{T}(r,n,d)$ in the "easy" cases $r \le 3$, and $(n,d) = (2,1)$ and $(r,n,d) = (4,2,2)$, and discuss $(n,d) = (\ge 3, 1)$. We also show that $\{1,2,3\} \notin \mathcal{T}(4,n,d)$. In section four we work out some concrete tickets. The most dysfunctional family we have found is $F \in \mathcal{F}(2k,2,2)$ for which $|T(F)| = 3k-3$ (and $\overline{m}(F) = 4k-4$); see Example 8. For each integer a, we give $F_a \in \mathcal{F}(a+2,2,a)$ so that $T(F_a)$ consists precisely of the divisors of a. We also give explicit $F, F' \in \mathcal{F}(6,2,2)$ with $T(F) = \{1,2,8\}$ and $T(F') = \{1,2,3,4,8,14\}$. These generalize (1.1). In fact, for every $v \ge 2$, there is a non-trivial identity equating two sums of the $(3v-1)$-st powers of v binary quadratic forms. We close the paper with generalizations, speculations, open questions and acknowledgments.

2. How long can a ticket be?

In this section we prove that $|T(F)| \le \binom{r-1}{2}$. The exposition is simplified by assuming that the f_j's are not homogeneous. We assume that $f_j = f_j(x)$, where $x = (x_1, \dots, x_n)$, although n does not play an explicit role in the proof. The proof is constructive in the sense that, for each F, we define a non-zero polynomial of degree $\binom{r-1}{2}$ in (m,x) which vanishes identically in x whenever $m \in T(F)$.

THEOREM 2.1. *Suppose $F = \{f_1, \dots, f_r\}$ is a set of polynomials over $\mathbb{C}$, no two of which are proportional, with* $\deg(f_j) \le d$. *Then $|T(F)| \le \binom{r-1}{2}$. If $d \le r-3$, then $|T(F)| < \binom{r-1}{2}$.*

PROOF. For a polynomial g and $k \ge 0$, let $(g)_k$ denote the degree k homogeneous part of g, so that $g = \sum_{k \ge 0} (g)_k$. If $\{g_1, \dots, g_r\}$ are linearly dependent polynomials, then $\sum_{j=1}^r \lambda_j g_j = 0$ implies that $\sum_{j=1}^r \lambda_j (g_j)_k = 0$ for all k. That is,

$$(2.1)\qquad \begin{pmatrix} (g_1)_0 & (g_2)_0 & \cdots & (g_r)_0 \\ (g_1)_1 & (g_2)_1 & \cdots & (g_r)_1 \\ \cdots & \cdots & \ddots & \cdots \\ (g_1)_{r-1} & (g_2)_{r-1} & \cdots & (g_r)_{r-1} \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Therefore, as a polynomial in x,

$$(2.2)\qquad W(g_1, \dots, g_r; x) := \begin{vmatrix} (g_1)_0 & (g_2)_0 & \cdots & (g_r)_0 \\ (g_1)_1 & (g_2)_1 & \cdots & (g_r)_1 \\ \cdots & \cdots & \ddots & \cdots \\ (g_1)_{r-1} & (g_2)_{r-1} & \cdots & (g_r)_{r-1} \end{vmatrix} = 0.$$

(This familiar and elementary Wronskian argument is assuredly not a *sufficient* condition for dependence. Given (2.2), the only null-vectors satisfying (2.1) might well have non-constant components. It might be the case that $\deg(g_j) < r-1$ for all j, rendering (2.2) trivial, and it might happen that $\sum_{j=1}^r \lambda_j g_j$ has terms of degree $\ge r$. Nevertheless, the weak necessary condition (2.2) will suffice for our needs. Wronskian arguments can also be found in **[11]** and **[15]**.)

We turn to F. Since f_i/f_j is not constant for $i \ne j$, there exists $k = k(i,j)$ so that

$$(2.3)\qquad \frac{\partial}{\partial x_k}\left(\frac{f_i}{f_j}\right) = \frac{1}{f_j^2}\left(f_j \frac{\partial f_i}{\partial x_k} - f_i \frac{\partial f_j}{\partial x_k}\right)$$

is not identically zero. For precision, let $k(i,j)$ be the smallest such index. Further, there exists a point $P \in \mathbb{C}^n$ which is *not* contained in the finite union

$$\left(\bigcup_{j=1}^{r}\{f_j=0\}\right)\bigcup\left(\bigcup_{1\le i<j\le r}\left\{f_j\frac{\partial f_i}{\partial x_{k(i,j)}}-f_i\frac{\partial f_j}{\partial x_{k(i,j)}}=0\right\}\right). \tag{2.4}$$

By translation, we may assume that $P=0$. If we now let $\gamma_j=(f_j(0))^{-1}$, and replace f_j by $\gamma_j f_j$, then we have changed neither the definition of the varieties in (2.4) nor $T(F)$. Accordingly, we may assume without loss of generality that $f_j(0)=1$ for all j. By evaluating (2.3) at $P=0$, we see that $\frac{\partial f_i}{\partial x_{k(i,j)}}(0)\neq\frac{\partial f_j}{\partial x_{k(i,j)}}(0)$, hence the first-order terms in the Taylor series of the f_j's at 0 are different. To emphasize this point, we write $(f_j)_1=L_j$.

We now compute $(f_j^m)_k$ explicitly:

$$\begin{aligned} f_j^m &= (1+L_j+(f_j)_2+\cdots+(f_j)_d)^m \\ &= \sum_{\substack{\ell_0+\cdots+\ell_d=m\\ \ell_0\ge 0,\ldots,\ell_d\ge 0}}\frac{m!}{\ell_0!\ldots\ell_d!}1^{\ell_0}L_j^{\ell_1}((f_j)_2)^{\ell_2}\ldots((f_j)_d)^{\ell_d}, \end{aligned} \tag{2.5}$$

and so $(f_j^m)_k$ will consist of those terms from (2.5) in which $\sum_{i=1}^d i\ell_i=k$. Write $(N)_s:=\frac{N!}{(N-s)!}=N(N-1)\cdots(N-(s-1))$. Since $\ell_0=m-\sum_{i=1}^d\ell_i$, we have

$$(f_j^m)_k=\sum_{\substack{\ell_1+\cdots+\ell_d\le m\\ \ell_1+\cdots+d\ell_d=k}}\frac{(m)_{\ell_1+\cdots+\ell_d}}{\ell_1!\ldots\ell_d!}L_j^{\ell_1}((f_j)_2)^{\ell_2}\ldots((f_j)_d)^{\ell_d}. \tag{2.6}$$

Consider (2.6) as presenting $(f_j^m)_k$ as a polynomial in m, whose coefficients are polynomials in x. From this perspective, each summand has m-degree $\ell_1+\cdots+\ell_d$. Since $\ell_1+2\ell_2+\cdots+d\ell_d=k$ is fixed, the maximum value of this m-degree is k, achieved uniquely (when $\ell_1=k$ and $\ell_i=0$, $i\ge 2$) in the term $\frac{(m)_k}{k!}L_j^k$. Thus,

$$(f_j^m)_k=\tfrac{L_j^k}{k!}\cdot m^k+\mathcal{O}_x(m^{k-1}),\qquad 0\le j\le r-1. \tag{2.7}$$

It is also easy to see that the term in $(f_j^m)_k$ with minimum m-degree occurs when $\ell_d=\lfloor k/d\rfloor$, and all other ℓ_i's vanish, except for $\ell_{k-d\lfloor\frac{k}{d}\rfloor}=1$, (unless $d\mid k$). Let $u(k,d):=\lfloor\frac{k-1}{d}\rfloor$. This smallest degree is $1+u(k,d)$ and implies that

$$m(m-1)\cdots(m-u(k,d))\mid(f_j^m)_k,\qquad 1\le k\le r-1.$$

(More directly, since f_j^m has degree $\le dm$, $(f_j^m)_k=0$ if $k>md$; that is, if $m\le\frac{k-1}{d}$.) Note that, in particular, $m\mid(f_j^m)_k$ if $k\ge 1$.

We apply (2.2) with $g_j=f_j^m$. Let $W(m;x):=W(f_1^m,\ldots,f_r^m;x)$. If $m\in T(F)$, then $W(m;x)=0$ as a polynomial in x. In view of (2.7), $W(m;x)$ equals

$$\begin{vmatrix} 1 & \cdots & 1\\ L_1\cdot m & \cdots & L_r\cdot m\\ \frac{L_1^2}{2!}\cdot m^2+\mathcal{O}_x(m) & \cdots & \frac{L_r^2}{2!}\cdot m^2+\mathcal{O}_x(m)\\ \vdots & \ddots & \vdots\\ \frac{L_1^{r-1}}{(r-1)!}\cdot m^{r-1}+\mathcal{O}_x(m^{r-2}) & \cdots & \frac{L_r^{r-1}}{(r-1)!}\cdot m^{r-1}+\mathcal{O}_x(m^{r-2}) \end{vmatrix}. \tag{2.8}$$

Then $W(m;x)$ has m-degree $\le \binom{r}{2}$, and the coefficient of $m^{\binom{r}{2}}$ is the Vandermonde determinant

$$\frac{1}{2!\cdots(r-1)!}\begin{vmatrix} 1 & \cdots & 1 \\ L_1(x) & \cdots & L_r(x) \\ \cdot & \ddots & \cdots \\ L_1^{r-1}(x) & \cdots & L_r^{r-1}(x) \end{vmatrix} = \frac{1}{2!\cdots(r-1)!}\prod_{1\le i<j\le r}(L_j(x)-L_i(x)).$$

Since the L_j's are distinct linear forms, there exists $y \in \mathbb{C}^n$ so that $L_i(y) \ne L_j(y)$ for $i \ne j$. Thus, $W(m;y)$ is a non-zero polynomial in m of exact degree $\binom{r}{2}$. Since m^{r-1} is a factor, $W(m;y)$ (and so $W(m;x)$) can have at most $\binom{r}{2} - (r-1) = \binom{r-1}{2}$ distinct factors of the shape $m - m_k$. (Recall that $T(F) \subseteq \{m_k\}$.) Moreover, the k-th row of (2.8) is divisible by $(m)_{1+u(k-1,d)}$, hence $W(m;y)$ is divisible by

$$\prod_{k=0}^{r-1}(m)_{1+u(k,d)} = \prod_{k=0}^{r-1} m(m-1)\ldots(m-u(k,d)) = \prod_{i=0}^{u(r-1,d)}(m-i)^{r-id-1}.$$

In particular, if $d \le r-3$, then $m^{r-1}(m-1)^2$ divides $W(m;y)$, so $|T(F)| < \binom{r-1}{2}$. Indeed, if $F \in \mathcal{F}(r,n,d)$, then

$$|T(F)| \le \binom{r}{2} - (r-1) - \sum_{i=1}^{u(r-1,d)}(r-2-id).$$

If $d = 2$, this bound works out to be $\lfloor r^2/4 \rfloor - 1$. For larger d it is $\approx \left(\frac{d-1}{2d}\right)r^2$. □

If $r = 3$, then Theorem 2.1 implies that $|T(F)| \le 1$; see Theorem 3.4 below.

If $r = 4$, then Theorem 2.1 implies that $|T(F)| \le 3$, and the bound is achieved in Example 1, and elsewhere. Example 5 will discuss $F \in \mathcal{T}(4,2,2)$ with $T(F) = \{1,2,4\}$. Theorem 3.7 will show that there is no family in any $\mathcal{F}(4,n,d)$ for which $T(F) = \{1,2,3\}$. (However, by Theorem 3.3, this is the ticket for any $F \in \mathcal{F}(5,2,1)$.)

Theorem 2.1 simplifies the task of finding the ticket: one may compute $W(m,x)$ and looks for factors in m. Once a finite set of candidate exponents is found, the dependence of the f_j^m's can be checked directly. We illustrate this in a special case, which will lead back to Example 1.

If $(n,d) = (1,2)$ and $r = 4$, then (2.5) becomes explicitly

$$\begin{aligned}(1+at+bt^2)^m &= 1 + mat + \left(\tfrac{m(m-1)}{2}a^2 + mb\right)t^2 \\ &+ \left(\tfrac{m(m-1)(m-2)}{6}a^3 + m(m-1)ab\right)t^3 + \ldots,\end{aligned} \tag{2.9}$$

(Note the factor of $(m)_0$ in $(f^m)_1$ and $(f^m)_2$, and the factor of $(m)_1$ in $(f^m)_3$.) After substituting (2.9) into (2.2) for $f_j(t) = 1 + a_jt + b_jt^2$, $1 \le j \le 4$, and taking common factors out of the rows, we find that

$$W(m;t) = \frac{m^3(m-1)}{12}t^6\begin{vmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_4 \\ (m-1)a_1^2 + 2b_1 & \cdots & (m-1)a_4^2 + 2b_4 \\ (m-2)a_1^3 + 6a_1b_1 & \cdots & (m-2)a_4^3 + 6a_4b_4 \end{vmatrix}. \tag{2.10}$$

Let $\Delta(m)$ denote the determinant in (2.10); if $1 \ne m_0 \in T(F)$, then $\Delta(m_0) = 0$.

EXAMPLE 1 (PART TWO). We dehomogenize (1.1) by setting $(x, y) \mapsto (1, t)$ and normalizing so that $f_j(0) = 1$. This gives

$$\begin{aligned} f_1(t) &= 1 + \sqrt{2}\, t - t^2, & f_2(t) &= 1 + i\sqrt{2}\, t + t^2, \\ f_3(t) &= 1 - \sqrt{2}\, t - t^2, & f_4(t) &= 1 - i\sqrt{2}\, t + t^2. \end{aligned} \tag{2.11}$$

Taking $a_j = i^{j-1}\sqrt{2}$ and $b_j = (-1)^j$ in (2.10), we find that $\Delta(m)$ is the determinant

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ \sqrt{2} & i\sqrt{2} & -\sqrt{2} & -i\sqrt{2} \\ 2(m-2) & -2(m-2) & 2(m-2) & -2(m-2) \\ 2\sqrt{2}(m-5) & -2i\sqrt{2}(m-5) & -2\sqrt{2}(m-5) & 2i\sqrt{2}(m-5) \end{vmatrix}.$$

A computation shows that $\Delta(m) = -128i(m-2)(m-5)$, which vanishes only for $m = 2, 5$. Remarkably, each root corresponds to a linear dependence among the $\{f_j^m\}$. If we replace $\sqrt{2}$ in (2.11) by a parameter $\mu > 0$, then the roots of $\Delta(m)$ work out to be $m = 1 + 2\mu^{-2}$, and $m = 2 + 6\mu^{-2}$. We shall show in Example 1 (Part Three) that, apart from $\mu = \sqrt{2}$, these roots correspond to a linear dependence only when $(\mu, m) = (\sqrt{6}, 3)$ and $(\sqrt{2/3}, 4)$. (See also (3.9) and (4.5).)

3. $\mathcal{T}(r, n, d)$ for small r, n, d

In this section, we describe $\mathcal{T}(r, n, d)$ in some simple cases.

3.1. Families of binary linear forms. It is very easy to see that $\mathcal{T}(r, 2, 1) = \{\{1, 2, \dots, r-2\}\}$. If $m \le r-2$, then $r > \binom{2+m\cdot 1-1}{2-1} = m+1$, hence $m \in T(F)$ is forced. Suppose $m = r-1$ and write $f_j(x, y) = \alpha_j x + \beta_j y$ for $1 \le j \le r$. Then the matrix giving $\{f_j^{r-1}\}$ with respect to the basis $\{\binom{r-1}{\ell} x^{r-1-\ell} y^\ell\}$ has Vandermonde determinant

$$\begin{vmatrix} \alpha_1^{r-1} & \alpha_1^{r-2}\beta_1 & \dots & \beta_1^{r-1} \\ \alpha_2^{r-1} & \alpha_2^{r-2}\beta_2 & \dots & \beta_2^{r-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_r^{r-1} & \alpha_r^{r-2}\beta_r & \dots & \beta_r^{r-1} \end{vmatrix} = \prod_{i<j} (\alpha_i\beta_j - \alpha_j\beta_i) \ne 0,$$

since the f_j's are pairwise non-proportional. It follows that $r - 1 \notin T(F)$. If $m \ge r$, then take $f_j(x, y) = \alpha_j x + \beta_j y$ for $r+1 \le j \le m+1$ so that $F' := F \cup \{f_{r+1}, \dots, f_{m+1}\}$ consists of $m+1$ pairwise non-proportional forms. Since $m \notin T(F')$ it follows that $m \notin T(F)$.

3.2. Families of linear forms in $n \ge 3$ variables. It follows from the foregoing that $\{1, \dots, r-2\} \in \mathcal{T}(r, n, 1)$ for $n \ge 3$. Can $\mathcal{T}(r, n, 1)$ contain anything else? We need a simple lemma.

LEMMA 3.1. *Suppose*

$$\sum_{j=1}^{r} \lambda_j \left(\alpha_{j1}x_1 + \dots + \alpha_{jn}x_n\right)^m = 0. \tag{3.1}$$

Then for every $\gamma = (\gamma_1, \dots, \gamma_n) \in \mathbb{C}^n$,

$$\sum_{j=1}^{r} \lambda_j \left(\sum_{k=1}^{n} \alpha_{jk}\gamma_k\right) \left(\alpha_{j1}x_1 + \dots + \alpha_{jn}x_n\right)^{m-1} = 0. \tag{3.2}$$

PROOF. Apply the differential operator $\frac{1}{m}\sum_{k=1}^{n}\gamma_k\frac{\partial}{\partial x_k}$ to (3.1). $\square$

LEMMA 3.2. *Suppose* $F = \{f_j\} \in \mathcal{F}(r,n,1)$ *and* $f_j(x) = \alpha_{j1}x_1 + \cdots + \alpha_{jn}x_n$ *for* $1 \le j \le r$.

(1) *If* $m \in T(F)$ *for* $F \in \mathcal{F}(r,n,1)$, *then* $m-1 \in T(F)$.
(2) *If* $F \in \mathcal{F}(r,n,1)$, *then* $\overline{m}(F) \le r-2$.

PROOF. (1) If $m \in T(F)$, then some non-trivial equation (3.1) holds, with, say, $\lambda_{j_0} \ne 0$. Since $f_{j_0} \ne 0$, there exists ℓ so that $\lambda_{j_0}\alpha_{j_0\ell} \ne 0$. By differentiating (3.1) with respect to x_ℓ, we see that $m-1 \in T(F)$.

(2) Suppose (3.1) holds. We claim by induction on $m \in T(F)$ that $m \le r-2$. If $m=1$, then the assumption that the forms are pairwise non-proportional implies that $r \ge 3$. Suppose now that the claim is true for $m-1$. There exists γ so that $\sum_{k=1}^n \alpha_{rk}\gamma_k = 0$, but $\sum_{k=1}^n \alpha_{jk}\gamma_k \ne 0$ for $j < r$ (as no α_j is proportional to α_r) and so the summand in (3.2) for $j=r$ disappears. By the inductive hypothesis, $m-1 \le r-3$, hence $m \le r-2$. $\square$

If $r > \binom{n+m-1}{n-1}$, then $\{1,\dots,m\}$ is forced to be in $T(F)$. Let $m(r,n)$ denote the largest integer m so that $r > \binom{n+m-1}{n-1}$, and note that $m(r,2) = r-2$. We have thus established the following theorem:

THEOREM 3.3. *If* $F \in \mathcal{F}(r,n,1)$, *then* $T(F) = \{1,\dots,k\}$, *where* $m(r,n) \le k \le r-2$.

EXAMPLE 3. Fix (r,n) and let $m = m(r,n)$, so that $\binom{n+m}{n-1} \ge r > \binom{n+m-1}{n-1}$. By Biermann's Theorem (see [**12**, p.31]),

$$\{(i_1x_1 + \cdots + i_nx_n)^{m+1} : 0 \le i_k \in \mathbb{Z},\ i_1 + \cdots + i_n = m+1\} \tag{3.3}$$

is a linearly independent set with $\binom{n+m}{n-1} \ge r$ elements. Let F be any subset of r of the linear forms in (3.3). Then $m+1 \notin T(F)$, but $\{1,\dots,m\}$ is forced to be in $T(F)$. Thus $T(F)$ is precisely $\{1,\dots,m(r,n)\}$ in this case.

We strongly suspect that every ticket allowed by Theorem 3.3 is achieved, since the extremes appear. We also strongly suspect that a proof of this result should not be difficult.

An alternative presentation of the foregoing can be made using "Serret's Theorem" (see [**1**] or [**12**, p.26]): given $\alpha_j \in \mathbb{C}^n$, $1 \le j \le r$, $\alpha_j = (\alpha_{j1},\dots,\alpha_{jn})$, the forms $\{(\sum_k \alpha_{jk}x_k)^m\}$ are linearly independent if and only if there exist "dual" forms $h_i(x_1,\dots,x_n)$ of degree m so that $h_i(\alpha_j) = 0$ if $i \ne j$, but $h_i(\alpha_i) \ne 0$. Theorem 2 in [**1**] implies Lemma 3.2(2).

3.3. Families of $r \le 3$ forms. This case is easily analyzed.

THEOREM 3.4. *For* $r \le 3$, $\mathcal{T}\{r,n,d\}$ *is given as follows:*

(1) $\mathcal{T}\{2,n,d\} = \{\emptyset\}$;
(2) $\mathcal{T}\{3,2,1\} = \{\{1\}\}$;
(3) $\mathcal{T}\{3,n,1\} = \{\emptyset,\{1\}\}$, *if* $n \ge 3$;
(4) $\mathcal{T}\{3,n,d\} = \{\emptyset,\{1\},\{2\}\}$, *if* $d \ge 2$.

PROOF. If $r=2$, $0 = \lambda_1 f_1^m + \lambda_2 f_2^m$ and $\lambda \ne (0,0)$, then f_1 and f_2 are proportional. If $r=3$ and $d=1$, then Theorem 3.3 and Example 3 imply (2) and (3). In any event, Theorem 2.1 implies that $|T(F)| \le 1$, "Fermat's Last Theorem" implies that $\overline{m}(F) \le 2$, and since $T(\{x^2-y^2, 2xy, x^2+y^2\}) = \{2\}$, it follows that $\{2\} \in \mathcal{T}\{3,n,d\}$ for $n, d \ge 2$. $\square$

3.4. Families of four binary quadratic forms. The simplest remaining case is $(r,n,d) = (4,2,2)$. The heavy lifting for this is done in the forthcoming [**13**], which identifies all families $F \in \mathcal{F}(4,2,2)$ which have $m \in T(F)$ with $m \ge 3$. Note also that $4 > \binom{2+2-1}{2-1}$, so $1 \in T(F)$ is forced, and $|T(F)| \le 3$ by Theorem 2.1.

If $T(F) \subseteq \{1,2\}$, then the possibilities are $\{1\}$ or $\{1,2\}$. These are achieved, respectively by

$$\{x^2, y^2, (x+y)^2, (x-y)^2\}, \qquad \{x^2, y^2, x^2+y^2, x^2-y^2\}.$$

Suppose $m \in T(F)$ with $m \ge 3$. Then we may scale $\{f_j\}$ so that

$$f_1^m + f_2^m = f_3^m + f_4^m, \qquad m \ge 3. \tag{3.4}$$

is an equation in binary quadratic forms. Write the common sum in (3.4) as p, then $p \ne 0$, $\{f_1^m, f_2^m\} \ne \{f_3^m, f_4^m\}$, and there do not exist $\alpha_j \in \mathbb{C}$ and $g \in \mathbb{C}[x,y]$ so that $\alpha_1^m + \alpha_2^m = \alpha_3^m + \alpha_4^m$ and $f_j = \alpha_j g$. This is the equation studied in [**13**], where the uniqueness assertions in the rest of this subsection are established. (Uniqueness is taken up to invertible linear changes of variable.)

EXAMPLE 4. For $m = 3$, the solutions to (3.4) satisfying the non-triviality conditions come from a single one-parameter family, first given, in a different form, by J. Young in 1832 (see [**3**, p.554]). For $\alpha \notin \{0,1,-1\}$ and $\omega = \zeta_3 = e^{2\pi i/3}$, let

$$\begin{aligned} f_1(x,y) &= \alpha x^2 - xy + \alpha y^2, \qquad & f_2(x,y) &= -x^2 + \alpha xy - y^2, \\ f_3(x,y) &= \omega\alpha x^2 - xy + \omega^2\alpha y^2, \qquad & f_4(x,y) &= -\omega x^2 + \alpha xy - \omega^2 y^2. \end{aligned} \tag{3.5}$$

Then

$$f_1^3(x,y) + \alpha f_2^3(x,y) = f_3^3(x,y) + \alpha f_4^3(x,y), \tag{3.6}$$

and it is not hard to show that $T(\{f_1,f_2,f_3,f_4\}) = \{1,3\}$ for every α. (Further, ω and ω^2 can be permuted in (3.5), giving a third pair of cubes in (3.6) with the same sum.)

EXAMPLE 5. For $m = 4$, there are two non-trivial solutions to (3.4). Let

$$\begin{aligned} f_1(x,y) &= x^2 + y^2, \qquad & f_2(x,y) &= \omega x^2 + \omega^2 y^2, \\ f_3(x,y) &= \omega^2 x^2 + \omega y^2, \qquad & f_4(x,y) &= xy. \end{aligned} \tag{3.7}$$

Then it is easy to verify that

$$f_1 + f_2 + f_3 = 0, \quad f_1^2 + f_2^2 + f_3^2 = 6f_4^2, \quad f_1^4 + f_2^4 + f_3^4 = 18 f_4^4.$$

It follows from Theorem 2.1 that $T(\{f_1,f_2,f_3,f_4\}) = \{1,2,4\}$. The "obvious" generalization of (3.7) is presented in Example 8.

After taking the linear transformation $(x,y) \mapsto (i(x-\omega y), x - \omega^2 y)$ in (3.7) and scaling, we obtain an equivalent version of F in $\mathbb{Z}[x,y]$:

$$\begin{aligned} f_1(x,y) &= x^2 + 2xy, \qquad & f_2(x,y) &= x^2 - y^2, \\ f_3(x,y) &= 2xy + y^2, \qquad & f_4(x,y) &= x^2 + xy + y^2. \end{aligned} \tag{3.8}$$

EXAMPLE 6. The other solution to (3.4) for $m = 4$ gives a family with ticket $\{1, 4\}$:

$$\sum_{\pm}(\sqrt{3}\,x^2 \pm \sqrt{2}\,xy - \sqrt{3}\,y^2)^4 = \sum_{\pm}(\sqrt{3}\,x^2 \pm i\sqrt{2}\,xy + \sqrt{3}\,y^2)^4. \tag{3.9}$$

This example corresponds to $(\mu, m) = (\sqrt{2/3}, 4)$ in Example 1 (Part Two).

The only solution to (3.4) for $m = 5$ is the family discussed in Example 1.

We summarize this discussion with a result whose proof relies on [**13**].

THEOREM 3.5.

$$\mathcal{T}(4, 2, 2) = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 2, 4\}, \{1, 2, 5\}\}.$$

Regarding $\mathcal{T}(4, 2, d)$ for larger d, Example 13 shows that $\{3\} \in \mathcal{T}(4, 2, 3)$ and Example 14 shows that $\{4\} \in \mathcal{T}(4, 2, 7)$.

3.5. If $r = 4$, then $\{1, 2, 3\}$ is not a ticket. We begin with a lemma.

LEMMA 3.6. *Suppose $\{f_j\} \in \mathcal{F}(r, n, d)$ is two-dimensional; that is, there exist f and g, not proportional, so that $f_j = \alpha_j f + \beta_j g$, $1 \le j \le r$. If $f_j' = \alpha_j x + \beta_j y$, then $T(\{f_j\}) = T(\{f_j'\})$. In particular, $T(\{f_j\}) \subseteq \{1, \dots, r-2\}$.*

PROOF. One inclusion is obvious. For the other, since no two f_j's are proportional, the same can be said about the (α_j, β_j)'s. Suppose $\sum_j \lambda_j f_j^m = 0$ and let $P(x, y) = \sum_j \lambda_j(\alpha_j x + \beta_j y)^m$, so that $0 = P(f, g)$. If $P = 0$, then $m \in T(\{f_j'\})$. Otherwise, $P(x, y) = \prod_i(\gamma_i x - \delta_i y)$ splits into linear factors, and $P(f, g) = 0$ implies that f and g are proportional, a contradiction. $\square$

THEOREM 3.7. *For every (n, d), $\{1, 2, 3\} \notin \mathcal{T}(4, n, d)$.*

PROOF. Let $F = \{f_1, f_2, f_3, f_4\}$ and suppose there are three non-trivial equations

$$0 = \lambda_{11} f_1 + \lambda_{12} f_2 + \lambda_{13} f_3 + \lambda_{14} f_4, \tag{3.10}$$

$$0 = \lambda_{21} f_1^2 + \lambda_{22} f_2^2 + \lambda_{23} f_3^2 + \lambda_{24} f_4^2, \tag{3.11}$$

$$0 = \lambda_{31} f_1^3 + \lambda_{32} f_2^3 + \lambda_{33} f_3^3 + \lambda_{34} f_4^3. \tag{3.12}$$

If the f_j's were to satisfy a linear relation different from (3.10), then F would be two-dimensional and Lemma 3.6 would imply $3 \notin T(F)$. Note also that Theorem 3.4 implies that $\lambda_{3j} \ne 0$ for all j.

Suppose first that one of λ_{1k}'s equals zero, say $\lambda_{14} = 0$. Then after scaling the f_j's, we can assume that $f_1 + f_2 = f_3$, and by Theorem 2.1 with $r = 3$, $\lambda_{2j} \ne 0$. Thus, after dividing by $\lambda_{\ell 4}$, and relabeling, (3.11) and (3.12) imply that

$$\beta_{21} f_1^2 + \beta_{22} f_2^2 + \beta_{23}(f_1 + f_2)^2 = f_4^2, \tag{3.13}$$

$$\beta_{31} f_1^3 + \beta_{32} f_2^3 + \beta_{33}(f_1 + f_2)^3 = f_4^3. \tag{3.14}$$

If $\beta_{21} u^2 + \beta_{22} v^2 + \beta_{23}(u + v)^2$ were a square, then (3.13) would imply a linear relation among f_1, f_2 and f_4, different from (3.10) and as noted above, this would be a contradiction. Otherwise, (3.13) and (3.14) together imply that

$$\left(\beta_{21} f_1^2 + \beta_{22} f_2^2 + \beta_{23}(f_1 + f_2)^2\right)^3 = \left(\beta_{31} f_1^3 + \beta_{32} f_2^3 + \beta_{33}(f_1 + f_2)^3\right)^2. \tag{3.15}$$

Since f_1 and f_2 are not proportional, (3.15) and the argument of Lemma 3.6 imply that

$$\left(\beta_{21}u^2+\beta_{22}v^2+\beta_{23}(u+v)^2\right)^3=\left(\beta_{31}u^3+\beta_{32}v^3+\beta_{33}(u+v)^3\right)^2. \tag{3.16}$$

But if $\Phi = G^3 = H^2$, then any irreducible factor of Φ must occur to the sixth power. Thus, (3.16) implies that $\beta_{21}u^2+\beta_{22}v^2+\beta_{23}(u+v)^2$ is a square, a contradiction.

Therefore, we may assume that $\lambda_{1k}\neq 0$, and so after scaling, $f_4 = f_1+f_2+f_3$ and

$$\begin{aligned}\beta_{21}f_1^2+\beta_{22}f_2^2+\beta_{23}f_3^2+\beta_{24}(f_1+f_2+f_3)^2&=0,\\ \beta_{31}f_1^3+\beta_{32}f_2^3+\beta_{33}f_3^3+\beta_{34}(f_1+f_2+f_3)^3&=0.\end{aligned} \tag{3.17}$$

By Bezout's Theorem, the intersection of the two curves

$$\begin{aligned}G_2(u,v,w) &:= \beta_{21}u^2+\beta_{22}v^2+\beta_{23}w^2+\beta_{24}(u+v+w)^2=0,\\ G_3(u,v,w) &:= \beta_{31}u^3+\beta_{32}v^3+\beta_{33}w^3+\beta_{34}(u+v+w)^3=0\end{aligned}$$

is (projectively) at most six lines, unless the curves share a component. Since (f_1,f_2,f_3) parameterizes the intersection by (3.17) and no two f_j are proportional, either $G_2 \mid G_3$ or both share a linear factor ℓ. However, if $G_2=\ell_1\ell_2$ for linear ℓ_j, then $G_2(f_1,f_2,f_3)=0$ implies that $\ell_j(f_1,f_2,f_3)=0$ for some j; this is different from $f_4=f_1+f_2+f_3$ and gives a contradiction as before.

The only remaining possibility is that $G_2 \mid G_3$ and G_2 is irreducible. After relabeling once again, we see that this case is

$$\begin{aligned}\left(\sigma_1u^2+\sigma_2v^2+\sigma_3w^2+2\sigma_4(uv+uw+vw)\right)&\left(\gamma_1u+\gamma_2v+\gamma_3w\right)\\ &=\tau_1u^3+\tau_2v^3+\tau_3w^3+\\ \tau_4(3u^2v+3uv^2+3uw^2+6uvw&+3uw^2+3v^2w+3vw^2).\end{aligned} \tag{3.18}$$

Since $\beta_{3j}\neq 0$, we may assume in (3.18) that $\tau_4\neq 0$ (hence $(\gamma_1,\gamma_2,\gamma_3)\neq(0,0,0)$) and that $\tau_j\neq\tau_4$ for $j=1,2,3$. By considering the coefficients of $u^2v, u^2w, uv^2, v^2w, uw^2, vw^2$ and uvw in (3.18), we find that

$$\begin{aligned}3\tau_4 = 2\gamma_1\sigma_4+\gamma_2\sigma_1 = 2\gamma_1\sigma_4+\gamma_3\sigma_1 &= 2\gamma_2\sigma_4+\gamma_1\sigma_2 = 2\gamma_2\sigma_4+\gamma_3\sigma_2\\ &= 2\gamma_3\sigma_4+\gamma_1\sigma_3 = 2\gamma_3\sigma_4+\gamma_2\sigma_3 = (\gamma_1+\gamma_2+\gamma_3)\sigma_4.\end{aligned} \tag{3.19}$$

Since $\tau_4\neq 0$, it follows that $\sigma_4\neq 0$. It follows immediately from (3.19) that

$$0=(\gamma_2-\gamma_3)\sigma_1=(\gamma_3-\gamma_1)\sigma_2=(\gamma_1-\gamma_2)\sigma_3. \tag{3.20}$$

If $\gamma_1=\gamma_2=\gamma_3:=\gamma\neq 0$, then (3.19) reduces to

$$3\tau_4=\gamma(\sigma_1+2\sigma_4)=\gamma(\sigma_2+2\sigma_4)=\gamma(\sigma_3+2\sigma_4)=3\gamma\sigma_4.$$

This implies that $\sigma_1=\sigma_2=\sigma_3=\sigma_4:=\sigma$, so $G_2(u,v,w)=(u+v+w)^2$, a contradiction.

If the γ_j's are not all equal, then after permutation of indices if necessary, we may assume that $\gamma_1\neq\gamma_2$ and $\gamma_1\neq\gamma_3$, hence $\sigma_2=\sigma_3=0$ by (3.20). Then (3.19) becomes

$$3\tau_4=2\gamma_1\sigma_4+\gamma_2\sigma_1=2\gamma_1\sigma_4+\gamma_3\sigma_1=2\gamma_2\sigma_4=2\gamma_3\sigma_4=(\gamma_1+\gamma_2+\gamma_3)\sigma_4.$$

Thus $\gamma_2=\gamma_3$, and so $2\gamma_2\sigma_4=(\gamma_1+\gamma_2+\gamma_3)\sigma_4$ implies $\gamma_1=0$. It then follows that $\sigma_1=2\sigma_4$, hence $G_2(u,v,w)=2\sigma_4(u+v)(u+w)$, a final contradiction. □

4. A few interesting tickets

The examples in this section indicate some of the diversity that is possible in tickets of indecomposable families. They are inspired, for the most part, by the examples from [**13**]. The families consist of binomials or highly symmetric trinomial binary forms, and rely heavily on the orthogonality properties of roots of unity.

Example 8 presents highly dysfunctional families $F \in \mathcal{F}(2v+2,2,2)$ with $|T(F)| = 3v$. Example 9 gives families $F \in \mathcal{F}(r,2,2)$ so that $T(F)$ contains $\{1,\dots,r-2\}$ as well as $r+s$, for any single integer s, $2 \le s \le r-1$. This is less dysfunctional than the previous example, but with a larger jump. The families in Example 10 are not dysfunctional, but have an even larger jump; for example, $\{1,2,8\} \in \mathcal{T}(6,2,2)$. One special case combines Examples 9 and 10 to show that $\{1,2,3,4,8,14\} \in \mathcal{T}(6,2,2)$. Example 11 presents $F \in \mathcal{F}(a+2,2,a)$ so that $T(F)$ consists precisely of the divisors of a. Example 12 combines Examples 7 and 11 and includes Molluzzo's example showing that $\overline{m}_r \ge \lfloor r^2/4 \rfloor - 1$. Example 13 verifies the claim from the Introduction that $\{m\} \in \mathcal{T}(m+1,2,m)$, while Example 14, due to Euler, shows that $\{4\} \in \mathcal{T}(4,2,7)$.

For integral $q \ge 2$, write $\zeta_q = e^{\frac{2\pi i}{q}}$. We shall say that a set of polynomials $\{f_0,\dots,f_{q-1}\}$ is *q-cyclotomic* on $\{g_0,\dots,g_{q-1}\}$ if

$$f_j = \sum_{k=0}^{q-1} \zeta_q^{jk} g_k, \qquad 0 \le j \le q-1, \tag{4.1}$$

where the g_k's involve disjoint sets of monomials. Note that, if $\{f_j\}$ is q-cyclotomic on $\{g_k\}$, then $\{f_j^m\}$ is q-cyclotomic on $\{g_{m,k}\}$, where

$$g_{m,k} = \sum_{\sum i_j \equiv k \mod q} g_{i_1}\cdots g_{i_m}, \tag{4.2}$$

provided the $g_{m,k}$'s involve disjoint monomials. This will occur if, for example, $f_j = f_j(x,y)$ and all terms in g_i have y-degree congruent to i (mod q).

LEMMA 4.1. *If $\{f_0,\dots,f_{q-1}\}$ is q-cyclotomic on $\{g_0,\dots,g_{q-1}\}$, then*

$$Span(f_0,\dots,f_{q-1}) = Span(g_0,\dots,g_{q-1}).$$

In particular, $\{f_j\}$ is linearly dependent if and only if some $g_k = 0$.

PROOF. By the orthogonality properties of roots of unity, (4.1) inverts to

$$g_\ell = \frac{1}{q}\sum_{j=0}^{q-1} \zeta_q^{-j\ell} f_j, \qquad 0 \le \ell \le q-1. \tag{4.3}$$

Thus the two spans are equal. Since the g_k's involve different monomials, they can only be trivially dependent. □

EXAMPLE 1 (PART THREE). Continuing the discussion in Example 1 (Part Two), suppose

$$\begin{aligned} f_1(t) &= 1+\mu t - t^2, \qquad & f_2(t) &= 1 + i\mu t + t^2, \\ f_3(t) &= 1-\mu t - t^2, \qquad & f_4(t) &= 1 - i\mu t + t^2. \end{aligned} \tag{4.4}$$

That is, $F = \{f_j\}$ is 4-cyclotomic on $\{1, \mu t, -t^2, 0\}$. To ensure pairwise non-proportionality in (4.4), we require $\mu \neq 0$. Suppose $1 < m \in T(F)$. Then it follows from Lemma 4.1 that $g_{m,k} = 0$ for some k. But for $m > 1$ and integral v,

$$g_{m,0} = 1 + \dots, \qquad g_{m,1} = m\mu t + \dots,$$
$$g_{2v+1,2} = \dots + t^{4v+2}, \qquad g_{2v,3} = \dots - 2v\mu t^{4v-1},$$

and since these $g_{m,k}$'s all have at least one non-zero term, the only $g_{m,k}$'s which might vanish are $g_{2v,2}$ and $g_{2v+1,3}$. We have

$$\begin{aligned} g_{2,2}(t) &= (\mu^2 - 2)t^2, \qquad g_{3,3}(t) = (\mu^3 - 6\mu)t^3, \\ g_{4,2}(t) &= (6\mu^2 - 4)(t^2 + t^6), \qquad g_{5,3}(t) = (10\mu^3 - 20\mu)(t^3 + t^7), \\ g_{6,2}(t) &= (15\mu^2 - 6)t^2 + (\mu^6 - 30\mu^4 + 90\mu^2 - 20)t^6 + (15\mu^2 - 6)t^{10}, \\ g_{7,3}(t) &= (35\mu^3 - 42\mu)t^3 + (\mu^7 - 42\mu^5 + 210\mu^3 - 140\mu)t^7 + (35\mu^3 - 42\mu)t^{11}. \end{aligned} \tag{4.5}$$

We see from (4.5) that $g_{m,k} = 0$ for $m \leq 7$ only in the following cases; $\mu^2 = 2$ and $m = 2$ or 5; $\mu^2 = 6$ and $m = 3$; and $\mu^2 = 2/3$ and $m = 4$. (It is evident that $g_{6,2}$ and $g_{7,3}$ can never vanish identically. Green's bound implies that we need only check $m \leq 8$; the computation of $g_{8,2}$ is left to the reader.)

For $\mu = \sqrt{2}$, we've already discussed F in Example 1 (Part Two). (This includes the seemingly accidental $g_{2,2} \mid g_{5,3}$.)

If $\mu = \sqrt{2/3}$, then after some simplification, we obtain (3.9).

If $\mu = \sqrt{6}$, then after homogenizing and inverting by (4.2), we obtain the identity

$$\begin{aligned} 6\sqrt{6}(x^5y + xy^5) &= (x^2 + \sqrt{6}xy - y^2)^3 - (x^2 - \sqrt{6}xy - y^2)^3 \\ &= (ix^2 - \sqrt{6}xy + iy^2)^3 - (ix^2 + \sqrt{6}xy + iy^2)^3. \end{aligned} \tag{4.6}$$

It turns out that $6\sqrt{6}(x^5y + xy^5)$ has four other representations as a sum of two cubes, involving 24-th roots of unity (see [**13**].) Noam Elkies notes that this follows from the many symmetries of the form $x^5y + xy^5$, whose zeros are the vertices of a regular octahedron in the Riemann sphere. It is possible to derive (4.6) from (3.5) using an unpleasant change of variables and an ugly choice of α.

EXAMPLE 7. Let $f_j(x, y) = x + \zeta_q^j y$. Then $\{f_0^m, \dots, f_{q-1}^m\}$ is q-cyclotomic on $\{g_{m,0}, \dots, g_{m,q-1}\}$, where

$$g_{m,k}(x, y) = \sum_{\substack{i \equiv k \mod q \\ 0 \leq i \leq m}} \binom{m}{i} x^{m-i} y^i.$$

If $m < q - 1$, then $g_{m,q-1} = 0$, hence $\{f_j^m\}$ is linearly dependent and so $m \in T(F)$. If $m \geq q - 1$, then $g_{m,k} \neq 0$, so $m \notin T(F)$. This is a special case of Theorem 3.3.

EXAMPLE 8. Suppose q is odd and let $f_j(x, y) = \zeta_q^j x^2 + \zeta_q^{-j} y^2$, $0 \leq j \leq q - 1$. (Since q is odd, no two f_j's are proportional.) Then

$$f_j^m(x, y) = \sum_{i=0}^{m} \binom{m}{i} \zeta_q^{(m-2i)j} x^{2m-2i} y^{2i},$$

so

$$g_{m,k}(x,y) = \sum_{m-2i\equiv k \mod q} \binom{m}{i} x^{2m-2i}y^{2i}. \tag{4.7}$$

Now let

$$F_q = \{f_0(x,y),\dots,f_{q-1}(x,y),xy\} \in \mathcal{F}(q+1,2,2).$$

(Without xy, this is essentially Example 7.) By Lemma 4.1,

$$\mathrm{Span}(f_0^m,\dots,f_{q-1}^m,(xy)^m) = \mathrm{Span}(g_{m,0},\dots,g_{m,q-1},(xy)^m). \tag{4.8}$$

It follows from (4.8) that $m \in T(F_q)$ if and only if for some i, either $g_{m,i} = 0$, or $g_{m,i}$ is a multiple of $(xy)^m$.

In the first case, if $m \ge q-1$, then there will exist i, $0 \le i \le m$, satisfying $m - 2i \equiv k \mod q$, and $g_{m,i} \ne 0$. If $m \le q-2$, then the equation $m - 2i \equiv m+2 \mod q$ implies that $i \equiv q-1 \mod q$, hence $g_{m,m+2} = 0$. Therefore, $T(F_q)$ contains $\{1,\dots,q-2\}$. (Alternatively, $f_j(x,y) = g_j(x^2,y^2)$ for linear g_j, and $m \le q-2$ is forced in $T(\{g_j\})$.)

In the second case, $(xy)^m$ can only occur in $g_{m,i}$ if m is even, $i = m/2$ and $k = 0$. Putting this into (4.7), we see that $(xy)^m$ is the only term in $g_{m,0}$ if and only if $i = m/2$ is the only solution to $2i \equiv m \mod q$ with $0 \le i \le m$, and this occurs if and only if $m/2 < q$; that is, $m < 2q$. Thus $T(F_q)$ contains the even integers $\{2,\dots,2q-2\}$. Writing $q = 2v+1$, we see that $r = |F_q| = 2v+2$ and

$$T(F_{2v+1}) = \{1,2,\dots,2v-1,2v,2v+2,\dots,4v-2,4v\}.$$

so that $|T(F_{2v+1})| = 3v = \frac{3}{2}r - 3$. The family defined in (3.8) is, in fact, F_3. The explicit linear relations are not very interesting:

$$\sum_{j=0}^{q-1} \left(\zeta_q^j x^2 + \zeta_q^{-j} y^2\right)^m = 0, \qquad \text{if } m < q \text{ is odd;}$$

$$\sum_{j=0}^{q-1} \left(\zeta_q^j x^2 + \zeta_q^{-j} y^2\right)^m = q\binom{m}{m/2}(xy)^m, \qquad \text{if } m < 2q \text{ is even.}$$

Example 9. This next example is a variation on Example 8, giving a smaller ticket, but one with a potentially larger gap. We no longer assume that q is odd. Let $\alpha \in \mathbb{C}$, let

$$f_{j,q,\alpha}(x,y) = \zeta_q^j x^2 + \alpha xy + \zeta_q^{-j} y^2, \qquad 0 \le j \le q-1, \tag{4.9}$$

and let

$$F_{q,\alpha} = \{f_{0,q,\alpha}(x,y),\dots,f_{q-1,q,\alpha}(x,y),xy\} \in \mathcal{F}(q+1,2,2).$$

Since

$$\left(\zeta_q^j x^2 + \alpha xy + \zeta_q^{-j} y^2\right)^m = \sum_{a+b+c=m} \frac{m!}{a!b!c!}\zeta_q^{j(a-c)}\alpha^b x^{2a+b}y^{b+2c},$$

by setting $b = m-a-c$ above, we see that

$$g_{m,k}(x,y) = \sum_{a-c\equiv k \mod q} \frac{m!}{a!c!(m-a-c)!}\alpha^{m-a-c}x^{m+(a-c)}y^{m-(a-c)}. \tag{4.10}$$

Again, $m \in T(F_{q,\alpha})$ if and only if $g_{m,k} = 0$ or is a multiple of $(xy)^m$. We shall not attempt a complete analysis of $T(F_{q,\alpha})$. Note, however, that the coefficient of a monomial in $g_{m,k}$ is a polynomial in α, and may vanish when α is suitably chosen.

If $m \le q-1$, then $a \equiv c \mod q$ and $m \ge |a-c|$ imply that $a = c$ so that (4.10) implies that

$$g_{m,0}(x,y) = \left(\sum_{a=0}^{\lfloor m/2 \rfloor} \frac{m!}{(a!)^2(m-2a)!} \alpha^{m-2a} \right) x^m y^m,$$

so $m \in T(F_{q,\alpha})$ for any α. Suppose now that $q \ge 3$ and $m = q+s$, $2 \le s \le q-1$. We fix $k = 0$. Then $a - c \equiv 0 \mod q$ implies that $a - c \in \{-q, 0, q\}$ and by (4.10), $g_{q+s,0}(x,y)$ is equal to

$$\left(\sum_{a=0}^{\lfloor s/2 \rfloor} \frac{(q+s)!}{a!(a+q)!(s-2a)!} \alpha^{s-2a} \right) (x^{s+2q}y^s + x^s y^{s+2q}) + B(\alpha)(xy)^{s+q}. \tag{4.11}$$

for some irrelevant polynomial $B(\alpha)$.

Since $s \ge 2$, there exists $\alpha = \alpha_0$ which kills the coefficient of $x^{s+2q}y^s + x^s y^{s+2q}$ in (4.11), so that $g_{q+s,0}$ is a multiple of $(xy)^{s+q}$. In this case,

$$\{1, \dots, q-1, q+s\} \subseteq T(F_{q,\alpha_0}).$$

We cannot rule out the possibility that $T(F_{q,\alpha_0})$ has other elements if α_0 is a root of other polynomials appearing in different $g_{m,k}$'s. Unless that happens, we have $r = |F_{q,\alpha_0}| = q+1$; if $s = q-1$ is maximal, then $\overline{m}(F_{q,\alpha_0}) \ge q+s = 2q-1$. Thus, $\overline{m}_r \ge 2r-3$, and this is larger than $\lfloor r^2/4 \rfloor - 1$ for $r \le 6$. The stronger bound $\overline{m}_6 \ge 14$ will follow from (4.15).

The simplest concrete realization of this phenomenon occurs when $q = 3$, $s = 2$ and $m = 5$. We have $\zeta_3 = \omega$ and (4.11) becomes

$$g_{5,0} = (5 + 10\alpha^2)(x^8y^2 + x^2y^8) + (a^5 + 20a^3 + 30a)x^5y^5.$$

Taking $\alpha_0 = \sqrt{-1/2}$, we define

$$\begin{aligned} f_{0,3,\alpha_0}(x,y) &= x^2 + \alpha_0 xy + y^2, \quad f_{1,3,\alpha_0}(x,y) = \omega x^2 + \alpha_0 xy + \omega^2 y^2, \\ f_{2,3,\alpha_0}(x,y) &= \omega^2 x^2 + \alpha_0 xy + \omega y^2, \qquad f_3(x,y) = xy. \end{aligned} \tag{4.12}$$

Then $T(F_{3,\alpha_0})$ contains $\{1,2,5\}$. After the linear change $(x,y) \mapsto (i(y-cx), x+cy)$ for $c = \frac{\sqrt{6}-\sqrt{2}}{2} = \sqrt{2-\sqrt{3}}$, (4.12) becomes a scaled and permuted version of (1.1). Example 1 strikes again!

Example 10. As a variation on the previous example, we again use (4.9), but specify $q = 2v \ge 4$ to be even and let

$$F'_{q,\alpha} = \{f_{0,q,\alpha}(x,y), \dots, f_{q-1,q,\alpha}(x,y)\} \in \mathcal{F}(2v,2,2).$$

Since $xy \notin F'_{q,\alpha}$, $m \in T(F'_{q,\alpha})$ only if there exists k so that $g_{m,k} = 0$. If $m \le v-1$, then $2v > \binom{2m+1}{1}$ so m is forced in $T(F'_{q,\alpha})$. With a careful choice of α, another exponent can be added to the ticket. We are interested in the largest possible jump. If $m = 3v-1$, then by (4.10), $g_{3v-1,v}(x,y)$ is equal to

$$\left(\sum_{a=0}^{v-1} \frac{(3v-1)!}{a!(a+v)!(2v-1-2a)!} \alpha^{2v-1-2a} \right) (x^{4v-1}y^{2v-1} + x^{2v-1}y^{4v-1}). \tag{4.13}$$

Since $v \ge 2$, there exists $\alpha = \alpha_0$ so that $g_{3v-1,v} = 0$; hence $\{1, ..., v-1, 3v-1\}$ is contained in $T(F'_{2v,\alpha_0})$. (As (4.13) gives an equation of degree $v-1$ satisfied by

α^2, we cannot expect "nice" roots α_0 for $v \ge 4$.) By applying the inversion formula (4.3) to $g_{3v-1,v} = 0$, we find that

$$0 = \sum_{j=0}^{2v-1} \zeta_{2v}^{-jv} f_{j,v,\alpha_0}^m = \sum_{j=0}^{2v-1} (-1)^j f_{j,v,\alpha_0}^m. \tag{4.14}$$

By transposing the terms in (4.14) with odd j, we obtain two sets of v quadratic forms with the property that the sum of their $3v-1$-st powers are equal.

The simplest case is $v = 2$, where (4.13) becomes $(10\alpha^3 + 20\alpha)(x^7y^3 + x^3y^7)$, so $\alpha_0 = \sqrt{-2}$. If we set $y \mapsto iy$, we get yet another appearance of Example 1.

If $v = 3$, then

$$g_{8,3}(x,y) = 56\alpha(3 + 5\alpha^2 + \alpha^4)(x^{11}y^5 + x^5y^{11}).$$

By setting $\alpha_0 = i\sqrt{\frac{5+\sqrt{13}}{2}}$ and noting $\zeta_6 = -\omega^2$, we see that (4.14) becomes, explicitly,

$$\begin{aligned}(x^2 + \alpha_0 xy + y^2)^8 + (\omega x^2 + \alpha_0 xy + \omega^2 y^2)^8 + (\omega^2 x^2 + \alpha_0 xy + \omega y^2)^8 &= \\ (x^2 - \alpha_0 xy + y^2)^8 + (\omega x^2 - \alpha_0 xy + \omega^2 y^2)^8 + (\omega^2 x^2 - \alpha_0 xy + \omega y^2)^8 &= \\ -3\left(\tfrac{1+\sqrt{13}}{2}\right)^4 x^2y^2(4x^{12} - 13^{3/2}x^6y^6 + 4y^{12}).&\end{aligned}$$

For $F = \{\omega^k x^2 \pm \alpha_0 xy + \omega^{-k} y^2\} \in \mathcal{F}(6,2,2)$, we have $T(F) = \{1,2,8\}$.

A computer check of $g_{3v-1,v}$ for $v \le 40$ shows that it is irreducible, except for $v = 5$ which has a factor of $\alpha^2 + 1$. Letting $\zeta = \zeta_5$, and transposing as in (4.14), we find:

$$\sum_{j=0}^{4} (\zeta^j x^2 + ixy + \zeta^{-j} y^2)^{14} = \sum_{j=0}^{4} (\zeta^j x^2 - ixy + \zeta^{-j} y^2)^{14} = 5^7 (xy)^{14} \tag{4.15}$$

It is miraculous, and wholly unexpected, that the common sum is also a 14-th power. In the language of Example 9, with $q = 5$, $g_{14,4}$ is a linear combination of $(x^{19}y^9 + x^9y^{19})$ and $(x^{24}y^4 + x^4y^{24})$, in which both coefficients have $\alpha^2 + 1$ as a factor.

Taking advantage of this opportunity, we let $f_j = \zeta^j x^2 + ixy + \zeta^{-j} y^2$, $0 \le j \le 4$ and $f_5 = \sqrt{-5}\, xy$, and define $\dot{F} = \{f_0, \dots, f_5\}$, then

$$0 = \sum_{j=0}^{4} f_j - \sqrt{5} f_5 = \sum_{j=0}^{5} f_j^2 = \sum_{j=0}^{4} f_j^3 + \sqrt{5} f_5^3 = \sum_{j=0}^{5} f_j^4 = \sum_{j=0}^{5} f_j^8 = \sum_{j=0}^{5} f_j^{14}. \tag{4.16}$$

A computer check, using $\overline{m}_6 \le 24$, shows no other relations. Thus, we have $T(\dot{F}) = \{1,2,3,4,8,14\}$ and $\overline{m}_6 \ge 14$.

Finally, if we put $(x,y) = (1,-1)$ into (4.15) and use the closed form of $\cos(\frac{2\pi k}{5})$, we derive a peculiar numerical identity:

$$2\left(\sqrt{5} + 1 + 2i\right)^{14} + 2\left(-\sqrt{5} + 1 + 2i\right)^{14} + (4 - 2i)^{14} = 20^7.$$

Example 11. This example is pleasantly uncomputational. Let

$$\widehat{F}_a = \{x^a + y^a, x^a, x^{a-1}y, \dots, xy^{a-1}, y^a\} \in \mathcal{F}(a+2, 2, a).$$

If $m \in T(\widehat{F}_a)$, then there is a non-trivial equation

$$\sum_{k=0}^{a} \lambda_k (x^{a-k}y^k)^m + \lambda_{a+1}(x^a + y^a)^m = 0.$$

But this is impossible if $\lambda_{a+1} = 0$, so we may scale to $\lambda_{a+1} = -1$ and consider

$$\sum_{k=0}^{a} \lambda_k (x^{a-k} y^k)^m = (x^a + y^a)^m = \sum_{\ell=0}^{m} \binom{m}{\ell} x^{ma-\ell a} y^{\ell a}.$$

This could hold if and only if $m \mid \ell a$ for each ℓ, $0 \le \ell \le m$; that is, if and only if m is a divisor of a. Thus, $T(\widehat{F}_a)$ consists of the divisors of a and $|T(\widehat{F}_a)|$ is the arithmetic function $d(a) \ll a$. This family is far from dysfunctional, but by taking $a = p^e$ for prime p, we see that $T(\widehat{F}_{p^e}) = \{1, p, p^2, \dots, p^e\}$. Thus, there is no bound on the ratio of consecutive elements in the ticket of an indecomposable family.

EXAMPLE 12. We combine Examples 7 and 11. For parameters $a, q \ge 2$, let

$$\widetilde{F}_{a,q} = \{x^a + y^a, x^a + \zeta_q y^a, \dots, x^a + \zeta_q^{q-1} y^a, x^a, x^{a-1}y, \dots, xy^{a-1}, y^a\}.$$

Then $\widetilde{F}_{a,q} \in \mathcal{F}(q + a + 1, 2, a)$. By Lemma 4.1, $m \in T(\widetilde{F}_{a,q})$ if and only if there exists k, $0 \le k \le q-1$, so that

$$\sum_{i \equiv k \mod q} \binom{m}{i} x^{(m-i)a} y^{ia}$$

is a linear combination of $\{x^{m(a-j)} y^{mj} : 0 \le j \le a\}$. For k, $0 \le k \le q-1$, let

$$S_k(m; a, q) = \{ia : i \equiv k \mod q,\ 0 \le i \le m\} = \{(k + bq)a : 0 \le b \le \lfloor \tfrac{m-k}{q} \rfloor\}.$$

and let $Z(m; a, q)$ denote the set of k for which $S_k(m; a, q)$ only contains multiples of m. Then $m \in T(\widetilde{F}_{a,q})$ if and only if some $Z(m; a, q)$ is non-empty.

If $m \le q-1$, then $S_0(m; a, q) = \{0\}$, so $m \in T(\widetilde{F}_{a,q})$. Since $S_0(m; a, q)$ consists of multiples of qa, if $m \mid qa$, then $0 \in Z(m; a, q)$, so $m \in T(\widetilde{F}_{a,q})$. If $|S_k(m; a, q)| \ge 2$ and $k \in Z(m; a, q)$, then m divides ka and $(k+q)a$, so m is a divisor of qa.

In the remaining case, $m \ge q$ is not a divisor of qa, but there exists k so that $m \mid ka$ and $S_k(m; a, q)$ is a singleton, so that $k \ge m - (q-1)$. The existence of such m depends on the arithmetic properties of a and q. If $a = q = p$ is prime, then no such m exists, and $T(\widetilde{F}_{p,p}) = \{1, \dots, p, p^2\}$. On the other hand, if $a = q = 6$, say, then it is not hard to show that $m = 8, 10$ satisfy the criteria and

$$T(\widetilde{F}_{6,6}) = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 18, 36\}.$$

Note that $F_{6,6}$ is (barely) dysfunctional.

Molluzzo ([**10**], see [**11**, p.485]) gives an equation, which when homogenized, is closely related to the family $\widetilde{F}_{a,q}$, with many monomials deleted. As we have seen,

$$\sum_{j=0}^{q-1} (x^a + \zeta_q^j y^a)^a = q \sum_{\ell=0}^{\lfloor a/q \rfloor} \binom{a}{\ell q} x^{a(a-q\ell)} y^{aq\ell}.$$

Accordingly, we let $t = \lfloor a/q \rfloor$ for short and define

$$\breve{F}_{a,q} = \{x^a + \zeta_q^j y^a\} \cup \{x^a, x^{a-q}y^q, \dots, x^{a-tq}y^{tq}\} \in \mathcal{F}(q + t + 1, 2, a),$$

so that $a \in T(\breve{F}_{a,q})$. The maximum possible value of a for fixed q, t occurs when $a = q(t+1) - 1$, and so it follows that

$$\overline{m}_{q+t+1} \ge q(t+1) - 1. \tag{4.17}$$

Fix $r = q + t + 1$. If $r = 2v$ is even, then (4.17) with $q = t + 1 = v$ shows that $\overline{m}_{2v} \ge v^2 - 1$; if $r = 2v + 1$ is odd, then (4.17) with $\{q, t + 1\} = \{v, v + 1\}$ shows that $\overline{m}_{2v+1} \ge v^2 + v - 1$. These combine to give the bound $\overline{m}_r \ge \lfloor r^2/4 \rfloor - 1$.

EXAMPLE 13. This example is another variation on Example 11. Recall the following family from the Introduction:

$$F_d^* := \{x^d + y^d, x^d + \zeta y^d, x^{d-1}y, \dots, xy^{d-1}\} \in \mathcal{F}(d + 1, 2, d),$$

where $\zeta = \zeta_d$. If $m \in T(F_d^*)$, then we have a non-trivial equation

$$\alpha(x^d + y^d)^m + \beta(x^d + \zeta y^d)^m + \sum_{j=1}^{d-1} \gamma_j (x^{d-j}y^j)^m = 0. \tag{4.18}$$

If $\alpha = \beta = 0$ in (4.18), then the γ_j's all vanish, so it is trivial. By considering the coefficients of x^{dm} and y^{dm}, we obtain the equations $\alpha + \beta = \alpha + \zeta^m \beta = 0$, hence $\beta = -\alpha$ and $\zeta^m = 1$, and so $m = sd$ for some integer s. We now consider the sum

$$\alpha\left((x^d + y^d)^{sd} - (x^d + \zeta y^d)^{sd}\right) + \sum_{j=1}^{d-1} \gamma_j (x^{d-j}y^j)^{sd}. \tag{4.19}$$

If $s > 1$, then the coefficient of $x^{sd^2-d}y^d$ in (4.19) will be $sd\alpha(1 - \zeta) \ne 0$. If $s = 1$, simply set $\alpha = 1$ and $\gamma_j = \binom{d}{j}(\zeta^j - 1)$ in (4.19) to set it equal to 0. We conclude that $T(F_d^*) = \{d\}$.

EXAMPLE 14. There are two famous parameterizations due to Euler which give singleton tickets. The Euler-Binet (complete) solution to (3.4) for $m = 3$ (see [**7**, p.200] gives $F \in \mathcal{F}(4, 3, 4)$ with $T(F) = \{3\}$. (But we already know that $F \in \mathcal{F}(4, 2, 3)$ has this ticket by the last example.)

Euler's binary septic solution to (3.4) for $m = 4$ ([**7**, p.201]) is

$$\begin{aligned}
f_1(x, y) &= x^7 + x^5y^2 - 2x^3y^4 + 3x^2y^5 + xy^6, \\
f_2(x, y) &= x^6y - 3x^5y^2 - 2x^4y^3 + x^2y^5 + y^7, \\
f_3(x, y) &= x^7 + x^5y^2 - 2x^3y^4 - 3x^2y^5 + xy^6, \\
f_4(x, y) &= x^6y + 3x^5y^2 - 2x^4y^3 + x^2y^5 + y^7.
\end{aligned}$$

Here, $F = \{f_j\} \in \mathcal{F}(4, 2, 7)$, and it can be shown that $T(F) = \{4\}$. This can be seen by a shortcut, avoiding the machinery of Theorem 2.1. Suppose $\sum_{j=1}^4 \lambda_j f_j^m = 0$. Then consideration of the terms x^{7m} and y^{7m} shows that $\lambda_3 = -\lambda_1$ and $\lambda_4 = -\lambda_2$. Hence by transposition, $\lambda_1(f_1^m - f_3^m) = \lambda_4(f_2^m - f_4^m)$. Evaluation at $(x, y) = (1, 1)$ implies that $\lambda_1(4^m - (-2)^m) = \lambda_4((-2)^m - 4^m)$, hence $\lambda_4 = -\lambda_1$, and the only possible relation is $f_1^m + f_2^m - f_3^m - f_4^m = 0$. This equation can now easily be checked for $m \le 8$. (The family F_4^* has five binary quartic forms; the ticket $\{4\}$ appears here for a family with fewer forms, but in higher degree.)

It is apparently unknown whether there is a non-trivial solution to the equation $f_1^4 + f_2^4 = f_3^4 + f_4^4$ in real binary forms of degree d for $3 \le d \le 6$. It seems clear to the author that the vast, centuries-old literature of Diophantine parameterizations can be data-mined for many more interesting examples of tickets.

5. Generalizations, speculations and open questions

This final section collects a number of disconnected miscellaneous remarks.

There is no reason to restrict our attention to forms over $\mathbb{C}$; for any field k, one might just as easily define $\mathcal{F}_k(r,n,d)$, where the forms have coefficients in k. It would be particularly interesting to study these for $k = \mathbb{Q}$ or $\mathbb{R}$. It is proved in [**13**] that there is no solution to (3.4) for real polynomials when $m = 5$. Thus, $(1,2,5) \notin \mathcal{T}_{\mathbb{R}}(4,2,2)$; (3.8) shows that $(1,2,4) \in \mathcal{T}_{\mathbb{Q}}(4,2,2)$. The forms in the highly dysfunctional family F_q in Example 8 are $\mathbb{R}$-combinations of x^2+y^2, $i(x^2-y^2)$ and xy, and hence can be made real by taking $(x,y) \mapsto (x+iy, x-iy)$. It seems difficult to determine when a given family of forms can be made real or rational by an appropriate linear change of variables. This is probably a deep question.

One can also sharpen the definition of $T(F)$. Let

$$\delta_m(F) = |F| - \dim(\operatorname{span}(\{f_j^m\}),$$

so that $T(F) = \{m : \delta_m(F) > 0\}$.

Conjecture 5.1.

$$\sum_{m=1}^{\infty} \delta_m(F) \le \binom{r-1}{2}. \tag{5.1}$$

Conjecture 5.1 implies Theorem 2.1 of course, and is valid for the examples given where $|T(F)| = \binom{r-1}{2}$ for $r = 3,4$. Further, if $(n,d) = (2,1)$, then $\delta_m(F) = r-(m+1)$ for $m \le r-2$, and (5.1) is sharp.

We can weaken Conjecture 1.1 enough to make it very plausible: suppose $A = \{m_k\}$ is finite and $m' \notin A$. Does there exist indecomposable F so that $A \subseteq T(F)$ and $m' \notin T(F)$? If not, then the linear dependence of $\{f_j^{m_k}\}$ forces the dependence of $\{f_j^{m'}\}$. This seems unlikely.

Example 1 (Part Four). We return to our favorite example one more time. Consider the intersection of the plane $M_1(t) = 0$ and the conic $M_2(t) = 0$. Then $t_4 = -(t_1+t_2+t_3)$, and so

$$t_1^2+t_2^2+t_3^2+(-(t_1+t_2+t_3))^2 = 2(t_1^2+t_2^2+t_3^2+t_1t_2+t_1t_3+t_2t_3) = 0. \tag{5.2}$$

It is not difficult to diagonalize (5.2) into

$$(t_1-t_2)^2+2(t_1+t_2)^2+(t_1+t_2+2t_3)^2 = 0. \tag{5.3}$$

Let

$$t_1-t_2 = x^2-y^2, \quad \sqrt{2}(t_1+t_2) = 2xy, \quad i(t_1+t_2+2t_3) = x^2+y^2$$

be the usual Pythagorean parameterization of (5.3). After solving for the t_i's, we discover that $t_j = f_j$, which is yet another way of deriving (1.1)!

The fact that $M_5(t) = 0$ as well can be explained in several ways. First,

$$t_1^5+t_2^5+t_3^5+(-(t_1+t_2+t_3))^5 =$$
$$-5(t_1+t_2)(t_1+t_3)(t_2+t_3)(t_1^2+t_2^2+t_3^2+t_1t_2+t_1t_3+t_2t_3),$$

so that (5.2) implies that $M_5(t) = 0$.

More generally, let e_k, $1 \le k \le 4$, denote the k-th elementary symmetric function in four variables. By Newton's Theorem, if $p(t_1,t_2,t_3,t_4)$ is a symmetric polynomial, then there is a polynomial P so that $p = P(e_1, e_2, e_3, e_4)$. If p is *any* symmetric form of degree five in four variables (not just M_5), then

$$p = \alpha_1 e_1^5 + \alpha_2 e_1^3 e_2 + \alpha_3 e_1^2 e_3 + \alpha_4 e_1 e_2^2 + \alpha_5 e_1 e_4 + \alpha_6 e_2 e_3. \tag{5.4}$$

If $M_1(t) = M_2(t) = 0$, then $e_1(t) = e_2(t) = 0$, and so $p = 0$ as well; p can be written as an element of the ideal (e_1, e_2) by solving for α_k in (5.4).

This construction generalizes. Suppose $r \geq 4$ and let A_r denote the set of integers which *cannot* be written in the form $a(r-1) + br$ for non-negative integers a and b. It is well-known that $|A_r| = \binom{r-1}{2}$ and the largest element in A_r is $r(r-1) - r - (r-1)$. Suppose

$$t_1^k + \cdots + t_r^k = 0, \qquad 1 \leq k \leq r-2. \tag{5.5}$$

Then the same argument given above implies that any homogeneous symmetric polynomial in r variables whose degree lies in A_r will vanish. If we could find pairwise non-proportional polynomials f_j, $1 \leq j \leq r$, satisfying (5.5), then we would thereby construct a family F of r polynomials with $T(F) = A_r$. This is a pipe dream. As several algebraic geometers have kindly pointed out, no such parameterization of (5.5) exists for $r \geq 5$ because it is then a smooth curve of positive genus. Many of the same people have also observed that this paper is "really" the study of rational curves lying on the intersection of several Fermat varieties of different degrees.

There is a different geometric interpretation of (1.1). Define the four pairs of complex numbers (β_j, γ_j) by the factorization $f_j(x, y) = \sigma_j(x - \beta_j y)(x - \gamma_j y)$. Under the standard stereographic projection of $\mathbb{C}$ to the unit sphere S^2, the four pairs (β_j, γ_j) map to the antipodal pairs of vertices of an inscribed cube. This is approach is somewhat reminiscent of Klein's classical work on the icosahedron. It would be very satisfying to understand (4.16) in the same detail as (1.1).

Example 8 shows that $|T(F)|$ can be as large as $\frac{3}{2}r - 3$. This is probably not maximal. Is $|T(F)| = \mathcal{O}(r)$? If not, what is the true growth rate? Can $c \cdot r^2$ be achieved for some $c > 0$? Does $\lim_{r \to \infty} r^{-2}\overline{m}_r$ exist?

Is it true that $T(F)$ contains at most $r - 2$ consecutive integers? This is true in all the dysfunctional families presented here, and would subsume Theorem 3.7.

Finally, we make the following definitions:

$$\mathcal{T}(r, n, \infty) = \bigcup_d \mathcal{T}(r, n, d) = \lim_{d \to \infty} \mathcal{T}(r, n, d);$$
$$\mathcal{T}(r, \infty, d) = \bigcup_n \mathcal{T}(r, n, d) = \lim_{n \to \infty} \mathcal{T}(r, n, d);$$
$$\mathcal{T}(r, \infty, \infty) = \bigcup_{n,d} \mathcal{T}(r, n, d) = \lim_{n,d \to \infty} \mathcal{T}(r, n, d).$$

Since $\mathcal{T}(r, \infty, \infty)$ is finite, it must actually be achieved by some $\mathcal{T}(r, n, d)$. Can we compute "minimal" $d(n, r)$ so that $\mathcal{T}(r, n, d(n, r)) = \mathcal{T}(r, n, \infty)$, "minimal" $n(d, r)$ so that $\mathcal{T}(r, n(d, r), d) = \mathcal{T}(r, \infty, d)$ or a family of "minimal" $(n(r), d(r))$'s so that $\mathcal{T}(r, n(r), d(r)) = \mathcal{T}(r, \infty, \infty)$?

6. Acknowledgments

I thank my colleagues Mike Bennett, Sean Sather-Wagstaff and Jack Wetzel, the organizers of the Analytic Number Theory, Commutative Ring Theory and

Geometric Potpourri seminars at UIUC, for their tolerance in letting me woodshed this material in their groups. I also thank Ricky Pollock, Marie-Francoise Roy and Micha Sharir for inviting me to speak at the DIMACS workshop on Algorithmic and Quantitative Aspects of Real Algebraic Geometry in Mathematics and Computer Science in March 2001.

I thank my colleagues Nigel Boston, Dan Grayson and Marcin Mazur for useful conversations. Marcin alerted me to the work of Mark Green. I would also like to thank Andrew Granville, Mark Green, Colleen Kilker, János Kollár and Gerry Myerson for helpful email correspondence. Finally, I am deeply grateful to Noam Elkies and Gary Gundersen for careful readings of the preprint and many useful suggestions.

More than is customary in such acknowledgments, the author wants to emphasize that he is solely responsible for any errors in content or aberrations in mathematical taste.

References

[1] A. Chlebowicz, A. Sładek, and M. Wołowiec-Musiał, *Automorphisms of certain forms of higher degree over ordered fields*, Linear Algebra Appl., **331** (2001), 145-153.

[2] H. Darmon and A. Granville, *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc., **27** (1995), 513-543.

[3] L. E. Dickson, *History of the Theory of Numbers, vol. II, Diophantine Analysis*, Chelsea, New York, 1966.

[4] M. L. Green, *Some Picard theorems for holomorphic maps to algebraic varieties*, Amer. J. Mathematics, **97** (1975), 43-75.

[5] G. G. Gundersen, *Meromorphic solutions of* $f^6 + g^6 + h^6 = 1$, Analysis (Munich), **18** (1998), 285-290.

[6] G. G. Gundersen, *Complex functional equations*, To appear in Univ. Joensuu Math. Dept. Report Series, in the proceedings of the summer school.

[7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th Ed., The Clarendon Press, Oxford Univeristy Press, New York, 1979.

[8] W. Hayman, *Warings Problem für analytische Funktionen*, Bayer. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. 1984, (1985), 1–13.

[9] W. Hayman, *Nevanlinna Theory 1945–1995*, XVIth Rolf Nevanlinna Colloquium (Joensuu, 1995) (I. Laine, O. Martio, eds.), W. de Gruyter, Berlin, New York, 1996, 1-11.

[10] J. Molluzzo, Doctoral Thesis, Yeshiva Univ., 1972.

[11] D. J. Newman and M. Slater, *Waring's Problem for the Ring of Polynomials*, J. Number Theory, **11** (1979), 477-487.

[12] B. Reznick, *Sums of even powers of real linear forms*, Mem. Amer. Math. Soc. Number 463, **96** (1992).

[13] B. Reznick, *Equal sums of higher powers of quadratic forms* in preparation. Seminar notes can be found at http://www.math.uiuc.edu/~reznick/92100notes.pdf.

[14] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York-Heidelberg, 1979.

[15] J. F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Bras. Math., **16**(2), (1985), 29-39.

Department of Mathematics, University of Illinois, Urbana, IL 61801
E-mail address: reznick@math.uiuc.edu