MATHEMATICAL CRYSTAL GROWTH I

D.A. KLARNER

Department of Mathematics, Technological University of Eindhoven, P.O. Box 513, Eindhoven, The Netherlands

Received 29 January 1980

Let $A, D$ be finite subsets of $\mathbb{Z}^k$ (the set of all $k$-tuples of integers), and consider the sequence of sets $(A, A + D, A + D + D, \ldots)$ which can be thought of as stages of growth in a crystal. One starts with a hub $A$ and adds increments equal to $D$. We represent finite subsets of $\mathbb{Z}^k$ by means of polynomials, and show that the sequence of polynomials corresponding to the crystal sequence is generated by a rational function. The proof is non-constructive.

Introduction

The idea for this paper began with a conjecture posed to me by Quinton Stout, one of my colleagues at SUNY Binghamton. He was interested in the spread of information in a large rectangular grid of computers which, for simplicity, is assumed unlimited in size. Communication between two computers takes place in one unit of time, and each computer is only capable of contacting others in a neighborhood $D$. This neighborhood pattern is the same for all the computers in the grid. At the start, one computer has some information, and in the first unit of time it sends this to its neighbors. Computers just contacted relay the information to their neighbors in the next unit of time. The process of spreading continues in this way. Let $f(t)$ denote the number of computers which have received the information after $t$ units of time. Stout conjectured that there exist integers $a, b, c, \ q$ such that $f(t) = at^2 + bt + c$ for all $t > q$. Another way to put this is that there exists a polynomial $p(z)$ of degree $q$ such that

$$\frac{p(z)}{(1-z)^3} = \sum_{t=0}^{\infty} f(t)z^t. \quad (1)$$

Stout's conjecture follows as a consequence of a far more general result proved in this paper.

First, we formulate our general problem in terms of mathematical crystal growth. The crystals are $k$-dimensional objects composed of $k$-dimensional unit cubes called cells. Cells are represented by elements of $\mathbb{Z}^k$, ($\mathbb{Z}$ is the set of integers, and $\mathbb{Z}^k$ is the set of $k$-tuples of integers), and a crystal is a subset of $\mathbb{Z}^k$. Let $A, D \subseteq \mathbb{Z}^k$ with $A, D$ non-empty, finite sets. Define a sequence of crystals $(C_t : t = 0, 1, \ldots)$ recursively by $C_0 = A$, and $C_{t+1} = C_t + D$ for $t = 0, 1, \ldots$, where the sum of two sets $X, Y \subseteq \mathbb{Z}^k$ is
defined $X + Y = \{x + y : x \in X, y \in Y\}$. (In this context, Stout's problem involves having $k = 2$, $A = \{(0, 0)\}$, and $D$ a finite subset of $\mathbb{Z}^2$ with $(0, 0) \in D$. Furthermore, the condition that $D$ be "two-dimensional" is that $D$ span $\mathbb{R}^2$. Finally, the interesting numbers are $f(t) = |C_t|$.) We will keep track of the elements of $C_t$ by making them correspond to the monomial summands of a polynomial in $k$ indeterminants which represents $C_t$. For each $v \in \mathbb{Z}^k$, let $w(v) = x^v = x_1^{v_1} \cdots x_k^{v_k}$ where $x_1, \ldots, x_k$, $v = (v_1, \ldots, v_k)$; also, if $C \subseteq \mathbb{Z}^k$, let $w(C) = \sum_{v \in C} w(v)$. (This sum is taken to be 0 if $C = \emptyset$.) Now we have the sequence $(w(C_t) : t = 0, 1, \ldots)$ and its generating function $F_{A,D}(x_1, \ldots, x_k, z) = F_{A,D}(x, z) = F(x, z)$ defined to be

$$F(x, z) = \sum_{i=0}^{\infty} w(C_t) z^t = \sum_{i=0}^{\infty} \sum_{v \in \mathbb{Z}^k} f(v, t) x^v z^t,$$

where $f(v, t)$ is the coefficient of $x^v$ in $w(C_t)$. Let $D = \{d_1, \ldots, d_n\}$ and let $\mathbb{N}$ denote the set of non-negative integers. Then $f(v, t)$ may be taken as

$$f(v, t) = \begin{cases} 1 & \text{if there exist } a \in A, t_1, \ldots, t_n \in \mathbb{N} \text{ such that } v = a + t_1 d_1 + \cdots + t_n d_n \text{ and } t = t_1 + \cdots + t_n, \\ 0 & \text{otherwise.} \end{cases}$$

The main result proved in this paper is that $F(x, z)$ is a rational function having a particular form. In fact, we are able to show that there exists a polynomial $G(x, z)$ such that

$$F(x, z) = \frac{G(x, z)}{H(x, z)} \quad \text{where } H(x, z) = \prod_{d \in D} (1 - x^d z).$$

The polynomials $G$ and $H$ may have common factors; in fact, we have found examples where they do. For each finite set $K \subseteq \mathbb{Z}^k$, let $\sum(K)$ denote the sum of the elements of $K$. If $K = \emptyset$, then $\sum(K)$ is taken to be the null vector $\theta = (0, 0, \ldots)$. Using this notation we have

$$H(x, z) = \sum_{K \subseteq \mathbb{N}} (-1)^{|K|} x^{\sum(K)} z^{|K|}.$$  

Let $g(v, t)$ and $h(v, t)$ denote the coefficients of $x^v z^t$ in $G(x, z)$ and $H(x, z)$ respectively for all $v \in \mathbb{Z}^k$, $t \in \mathbb{N}$. (Of course, if $G$ and $H$ are polynomials, this means $g(v, t)$ and $h(v, t)$ are almost always 0.) If (4) is multiplied through with $H$ as given in (5) and the coefficients of $x^v z^t$ are equated in the resulting expression, one gets

$$g(v, t) = \sum_{K \subseteq \mathbb{N}} (-1)^{|K|} f(v - \sum(K), t - |K|)$$

for all $v \in \mathbb{Z}^k$, $t \in \mathbb{N}$. If (6) is taken as the definition of $g(v, t)$, and it is shown that $g(v, t) = 0$ for all but a finite set of pairs $(v, t)$, then it follows that $G(x, z)$ is a polynomial and (4) is a consequence. This is the approach taken in our proof.

There are several interesting consequences of (4), one of which is a $k$-dimensional version of Stout's conjecture. Suppose $D = \{d_1, \ldots, d_n\}$ spans a vector space with dimension $m$ in $\mathbb{R}^k$, so $m \leq k$, and we can suppose without loss of generality that
$d_1, \ldots, d_m$ are linearly independent. Also, suppose $D$ contains the null vector $\theta$. Then for a fixed $a \in A$ and $t \in \mathbb{N}$ we can indicate a large set of distinct elements of $C_t$. Namely, all vectors $v = a + t_0 \theta + t_1 d_1 + \cdots + t_m d_m$ with $t_0, \ldots, t_m \in \mathbb{N}$ and $t_0 + \cdots + t_m = t$ are distinct elements of $C_t$. The number of these vectors is the number of compositions of $t$ into $m + 1$ non-negative parts which is $(t + m)^m$, so $C_t$ has at least $\theta(t^m)$ elements. On the other hand, no element of $C_t$ is longer than $r' + rt$ where $r'$ and $r$ are the lengths of the longest vectors in $A$ and $D$ respectively, so all the vectors in $C_t$ are contained in an $m$-dimensional cube with side $2(r' + rt)$. Hence, $C_t$ has no more than $\theta(t^m)$ elements, so $|C_t| = \theta(t^m)$. (We remark without proof that if $D$ does not contain the null vector, then $|C_t|$ is either $\theta(t^{m-1})$ or $\theta(t^m)$.) Now we use the generating function for $(|C_t| : t = 0, 1, \ldots)$ obtained from (4) by putting $x_1 = \cdots = x_k = 1$. Generally, $G(1, z)$ and $H(1, z)$ will have several common factors equal to $1 - z$, so the form is

$$\frac{E(z)}{(1 - z)^{m+1}} = \sum_{t=0}^{\infty} |C_t| z^t.$$  

where $1 - z$ is not a factor of the polynomial $E(z)$; that is, $E(1) \neq 0$. Development of $E(z)/(1 - z)^{m+1}$ into a power series gives

$$|C_t| = \frac{E(1) t^m}{m!} + B(t)$$  

where $B(t)$ is a polynomial with degree less than $m$. In fact, if $E(z) = e_0 + e_1 z + e_2 z^2 + \ldots$, then

$$|C_t| = e_0(m + t \choose m) + e_1(m + t - 1 \choose m) + e_2(m + t - 2 \choose m) + \ldots,$$  

for $t = 0, 1, \ldots$, which is a polynomial in $t$ of degree $m$ for all sufficiently large $t$.

Another interesting consequence of (4) is that the sequence of polynomials $(w(C_t) : t = 0, 1, \ldots)$ satisfies a difference equation. Put

$$H(x, z) = \sum_{t=0}^{\infty} H_t(x) z^t,$$  

then multiplying through (4) with $H(x, z)$ in this form yields

$$H_0(x) w(C_t) + \cdots + H_{|D|}(x) w(C_{t - |D|}) = 0$$  

for all sufficiently large $t$. There is another observation related to this one. Sequences of polynomials corresponding to crystals formed by taking the cross-sections of $C_t$ at a fixed hyperplane (say $x_1 = 4, x_2 = 0$) are also generated by rational functions. The appropriate generating functions are certain partial derivatives of $F$.

Our proof (given in the next section) that $g(v, t)$ is almost always $0$ is non-constructive. Initially, proving Stout's conjecture was our primary goal, and for this the non-constructive proof suffices. However, the generating function $F$ is clearly interesting and worthy of study all by itself. So a later discovery of a way to compute $F$ forms a sequel to this paper.
Proof that $F$ is rational

We fix $v \in \mathbb{Z}^k$, $t \in \mathbb{N}$ throughout this discussion; also, let $D = \{d_1, \ldots, d_n\}$. Suppose $L \subseteq K \subseteq D$, and $f(v - \Sigma(K), t - |K|) = 1$. Then there exist $a \in A$, $t_1, \ldots, t_n \in \mathbb{N}$ such that

\begin{align*}
    v - \Sigma(K) &= a + t_1d_1 + \cdots + t_nd_n, \\
    t - |K| &= t_1 + \cdots + t_n. 
\end{align*}

(12)

(13)

If $\Sigma(K \setminus L)$ is added to each side of (12) and $|K \setminus L|$ is added to each side of (13), we find integers $t'_1, \ldots, t'_n \in \mathbb{N}$ (in fact, $t_i \leq t'_i$ for $i = 1, \ldots, n$) such that

\begin{align*}
    v - \Sigma(L) &= a + t'_1d_1 + \cdots + t'_nd_n, \\
    t - |L| &= t'_1 + \cdots + t'_n.
\end{align*}

(14)

(15)

Hence, $L \subseteq K \subseteq D$ and $f(v - \Sigma(K), t - |K|) = 1$ implies $f(v - \Sigma(L), t - |L|) = 1$. This means the set of subsets $K \subseteq D$ such that $f(v - \Sigma(K), t - |K|) = 1$ forms a lower end in the partially ordered set of all subsets of $D$. Let $\mathcal{M}$ denote the set of maximal elements of this lower end. Explicitly,

\[
    \mathcal{M} = \{M \subseteq D : f(v - \Sigma(M), t - |M|) = 1, \text{ and } f(v - \Sigma(K), t - |K|) = 0 \text{ for all } K \}
\]

\[
    \text{with } M \subset K \subseteq D \}.
\]

Now we know which summands in (6) are non-zero. Let $\mathcal{M} = \{M_1, \ldots, M_m\}$, let $\mathcal{P}(X)$ denote the set of all subsets of a set $X$, and put $\mathcal{A} = \mathcal{P}(M_1) \cup \cdots \cup \mathcal{P}(M_m)$. Then

\[
    g(v, t) = \sum_{K \subseteq D} (-1)^{|K|}f(v - \Sigma(K), t - |K|) = \sum_{K \in \mathcal{M}} (-1)^{|K|}.
\]

(16)

The last sum in (16) is over a union of sets, so we can use the weighted version of the inclusion-exclusion formula (see Ryser [1]). The weight of a set $X$ is taken as $(-1)^{|X|}$, then

\[
    g(v, t) = \sum_{K \subseteq \mathcal{M}} (-1)^{|K|} = -\sum_{K \subseteq \mathcal{M}} (-1)^{|\cap \mathcal{A}|},
\]

(17)

where the second sum extends over all non-empty subsets $\mathcal{A}$ of $\mathcal{M}$. Here we have used the fact that if $\mathcal{A} = \{B_1, \ldots, B_i\} \subseteq \mathcal{M}$, then $\mathcal{P}(B_1) \cap \cdots \cap \mathcal{P}(B_i) = \mathcal{P}(B_1 \cap \cdots \cap B_i)$, and for any finite set $X$

\[
    \sum_{K \subseteq \mathcal{X}} (-1)^{|K|} = (1 - 1)^{|X|}.
\]

(18)

Now the right member of (17) hints why $g(v, t)$ might be 0. If $B_1 \cap \cdots \cap B_i \neq \emptyset$ for every non-empty collection $\mathcal{A} = \{B_1, \ldots, B_i\} \subseteq \mathcal{M}$, then every summand in (17) is 0. (Of course, $0^i = 0$ if $i \neq 0$, and $0^0 = 1$.) The maximal sets associated with $(v, t)$ may not have this non-trivial intersection property, but we will show that if $g(v, t) \neq 0$, then the “descendants” of $(v, t)$ come “nearer” to fulfilling this condition.

Let $V = V(A, D)$ denote the set of all pairs $(v, t)$, $v \in \mathbb{Z}^k$, $t \in \mathbb{N}$, such that there exist $a \in A$, $t_1, \ldots, t_n \in \mathbb{N}$ with $v = a + t_1d_1 + \cdots + t_nd_n$, $t = t_1 + \cdots + t_n$. We define a binary
relation $R = R(A,D)$ on $V$ with $(v,t) \rightarrow (v',t')$ a pair in the relation just when there exist $t_1, \ldots, t_n \in \mathbb{N}$ such that $v' = v + t_1d_1 + \cdots + t_nd_n$ and $t' = t + t_1 + \cdots + t_n$. This is the notion of "descendant." It is easy to check that $R$ is a transitive relation, but even more important, $R$ is a quasi-order. That is, for every infinite subset $S \subseteq V$ there exist two distinct elements $(v,t), (v',t') \in S$ with $(v,t) \rightarrow (v',t')$. One can deduce from this that $S$ contains an infinite subset $\{(v_1,t_1), (v_2,t_2), \ldots\}$ which forms a chain $(v_1, t_1) \rightarrow (v_2, t_2) \rightarrow \cdots$. Since we need this last property of quasi-orders, we will prove $R$ is a quasi-order.

Suppose $S \subseteq V$ is infinite and define a finite cover of $S$ as follows: for each $a \in A$, let $S_a = \{(v,t) \in S : (a,0) \rightarrow (v,t)\}$, then $\{S_a : a \in A\}$ is a finite cover of $S$. Since $S$ is infinite, one of the sets $S_a$ is infinite also, say $S_b$. For each $(v,t) \in S_b$, let $g(v,t) = (t_1, \ldots, t_n)$ where $(t_1, \ldots, t_n) \in \mathbb{N}^n$ is any one of the $n$-tuples such that $v = b + t_1d_1 + \cdots + t_nd_n$ and $t = t_1 + \cdots + t_n$. Now if $(v,t), (v',t')$ are distinct elements of $S_b$, then $g(v,t) \neq g(v',t')$. Hence, $g(S_b) = \{g(v,t) : (v,t) \in S_b\}$ is an infinite subset of $\mathbb{N}^n$. It is well-known that $\mathbb{N}^n$, ordered by $(i_1, \ldots, i_n) \leq (j_1, \ldots, j_n)$ when $i_h \leq j_h$ for $h = 1, \ldots, n$, is a quasi-order. So there exist distinct elements $(v,t), (v',t') \in S_b$ with $g(v,t) \leq g(v',t')$, and this means $g(v,t) \rightarrow g(v',t')$.

Suppose $(v,t), (v',t')$ are distinct elements of $V$, and let $\mathcal{A}'$ denote the set of maximal sets associated with $(v',t')$. We are going to show that if $g(v,t) \neq 0$ and $(v,t) \rightarrow (v',t')$, then $\mathcal{A}$ is dominated by $\mathcal{A}'$. (That is, every set in $\mathcal{A}$ is contained in some set in $\mathcal{A}'$, and $\mathcal{A} \neq \mathcal{A}'$.) Since $(v,t) \neq (v',t')$ and $(v,t) \rightarrow (v',t')$, there exists a non-empty subset $H \subseteq D$, say $H = \{d_1, \ldots, d_h\}$, and positive integers $i_1, \ldots, i_h \in \mathbb{P}$, so that

\begin{align*}
i_1d_1 + \cdots + i_hd_h & \leq u, \quad v + u - v', \\
i_1 + \cdots + i_h & = i', \quad t + i = i'.
\end{align*}

(19)  \hspace{1cm} (20)

Now

\begin{align*}
v' - \Sigma(K) & = b + j_1d_1 + \cdots + j_nd_n, \\
t' - |K| & = j_1 + \cdots + j_n.
\end{align*}

(21)  \hspace{1cm} (22)

and the existence of this representation proves $f(v' - \Sigma(K\cup H), t' - |K\cup H|) = 1$. Thus, $K \cup H \subseteq K'$ for some $K' \in \mathcal{A}'$.

We cannot have $K = K \cup H$ for all $K \in \mathcal{A}$ because $g(v,t) = 0$ in this case. (If $K = K \cup H$ for all $K \in \mathcal{A}$, we have $H \subseteq \bigcap \mathcal{A}$ for all non-empty $\mathcal{A} \subseteq \mathcal{A}$, and under these conditions $g(v,t) = 0$.) Hence, some element of $\mathcal{A}$ is properly contained in an element of $\mathcal{A}'$, so $\mathcal{A} \neq \mathcal{A}'$. This means $\mathcal{A}'$ dominates $\mathcal{A}$.

Before putting the capstone on the proof that $g(v,t)$ is almost always 0, we need one more observation. If $\mathcal{A}_0, \ldots, \mathcal{A}_h$ are antichains in $\mathcal{P}(D)$ ordered by set inclusion such that $\mathcal{A}_i$ dominates $\mathcal{A}_{i-1}$ for $i = 1, \ldots, h$, then $h \leq 2^{|D|}$. We leave this proof as a
recreation for the reader. Actually, all we require is that $h$ cannot be infinite, and this is obvious because $\mathcal{P}(D)$ has only a finite set of antichains.

Finally, we show $g(v, t)$ is almost always 0. Let $S = S(A, D)$ denote the set of all $(v, t)$ with $g(v, t) \neq 0$. It is easy to see that $S \subseteq V$. If $S$ is infinite, it follows from the fact that $R$ is a quasi-order that $S$ contains an infinite set $\{(v_1, t_1), (v_2, t_2), \ldots \}$ with $(b, 0) = (v_1, t_1) \rightarrow (v_2, t_2) \rightarrow \cdots$ for some $b \in A$. Let $\mathcal{M}_i$ denote the set of maximal sets associated with $(v_i, t_i)$ for $i = 1, 2, \ldots$. Since $g(v_i, t_i) \neq 0$ for $i = 1, 2, \ldots$, $\mathcal{M}_{i+1}$ dominates $\mathcal{M}_i$ for all $i \in \mathbb{P}$. This contradicts the fact that $\mathcal{P}(D)$ has only a finite set of antichains, so $S$ is finite. This completes the proof.

Note. My attention has been called to a recent paper of G.W. Peck: “Optimal spreading in an $n$-dimensional rectilinear grid”, to appear in Studies in Applied Mathematics, which concerns a similar problem setting, while dealing with different questions.

Reference