# Proofs of some divide-and-conquer generating functions

Ralf Stephan*

In this article, we give two independent proofs of the power series generating functions of the recurrence class $a_{2n} = \alpha a_n + c, a_{2n+1} = \alpha a_n + d$, one from the ground up, and one using a recently published lemma of the author.

Having motivated the search for ordinary generating functions of divide-and-conquer recurrences (and vice versa) earlier[S1], we state first the results of this article.

Let us acquire a symbol from Wilf[W] and define for a formal power series $f$ and a sequence $\{a_n\}_0^\infty$ that $f \overset{\text{ogf}}{\longleftrightarrow} \{a_n\}_0^\infty$ means $f(z) = \sum_j a_j z^j$. Throughout this article, let $\alpha, c, d$ be integers, with $|\alpha| > 0$.

**Theorem 1.** *The sequences*

$$e(\alpha, c, d; n): \qquad \{a_0 = 0,\ a_{2n} = \alpha \cdot a_n + c,\ a_{2n+1} = \alpha \cdot a_n + d\} \tag{0.1}$$

*satisfy*

$$\frac{1}{1-z} \sum_{k\geq 0} \frac{\alpha^k (d \cdot z^{2^k} + c \cdot z^{2^{k+1}})}{1 + z^{2^k}} \quad \overset{\text{ogf}}{\longleftrightarrow} \quad e(\alpha, c, d; n) \tag{0.2}$$

*and*

$$e(\alpha, c, d; n) \quad = \quad \begin{cases} (d-c) \cdot e_1(n) \ + \ c(\lfloor \log_2 n \rfloor + 1), & \alpha = 1, \\ (d-c) \sum_{i\geq 0} \alpha^i b_i \ + \ \dfrac{c\left(\alpha^{\lfloor \log_2 n \rfloor + 1} - 1\right)}{\alpha - 1}, & \textit{else}, \end{cases} \tag{0.3}$$

*where* $n = \sum 2^i b_i$ *and* $e_1(n) = \sum b_i$.

The first section contains the proof of all results by elementary means, and the second section proves (0.2) using a new lemma.

## 1. Bits and Pieces

Let $\alpha, c, d$ be integers, $|\alpha| > 0$. The sequences defined by

$$\begin{aligned} e(\alpha, c, d; n) &= 0, & n &= 0, \\ &= \alpha \cdot e(\alpha, c, d; n/2) + c, & n &= 2k, \quad (1.1)\\ &= \alpha \cdot e(\alpha, c, d; (n-1)/2) + d, & n &= 2k+1, \quad (1.2) \end{aligned}$$

include the ones- and zero-counting (and other well-known) sequences with

$$\begin{aligned} e_1(n) \quad &= \quad e(1, 0, 1; n) \quad = \quad \sum_{m\geq 0} [\, m\text{-th bit of } n \text{ exists and is set}\,], \\ e_0(n) \quad &= \quad e(1, 1, 0; n) \quad = \quad \sum_{m\geq 0} [\, m\text{-th bit of } n \text{ exists and is not set}\,]. \end{aligned}$$

In order to arrive at Theorem 1, we will prove generating functions with increasing complexity. For the purpose, it is necessary to be rigorous about bits. A number $n$, expressed in *the minimal binary representation*, has $\lfloor \log_2 n \rfloor + 1$ digits, called bits: a bit can exist or not, and it can be set or not set. Likewise, we would in decimal assume that 08 and 8 are different representations that amount to the same number. Let us define the following functions restricted on $m, n \geq 0$:

$$[\, m\text{-th bit of } n \text{ exists and is set}\,] = \begin{cases} 1 & n > 0 \ \texttt{\&\&}\ m \leq \lfloor \log_2 n \rfloor \ \texttt{\&\&}\ \text{bit is set}, \\ 0 & \textit{else}, \end{cases}$$

$$[\, m\text{-th bit of } n \text{ exists and is not set}\,] = \begin{cases} 1 & n > 0 \ \texttt{\&\&}\ m \leq \lfloor \log_2 n \rfloor \ \texttt{\&\&}\ \text{bit is not set}, \\ 0 & \textit{else}, \end{cases}$$

*mailto:ralf@ark.in-berlin.de

where '&&' denotes logical AND. The recurrence acts as the divide-and-conquer algorithm that, starting from an index $n$, reaches 0 using a path between the two recurrence branches. This path is identical to the minimal binary representation of $n$, when read from the least significant bit first, if one denotes branch (1.2) as 1 and (1.1) as 0.

**Lemma 1.** *For integer $m \geq 0$,*

$$\frac{1}{1-z} \cdot \frac{z^{2^m}}{1+z^{2^m}} \quad \overset{\text{ogf}}{\longleftrightarrow} \quad \{a_{m,n} = [\, m\text{-th bit of } n \text{ exists and is set}\,]\}. \tag{1.3}$$

*Proof.* For $m = 0$ we have the series $z/(1-z^2)$ which generates $\{0,1,0,1,\ldots\}$ because it consists of the partial sums (cf. the factor $1/(1-z)$) of the sequence $\{0,1,-1,1,-1,\ldots\}$ that is generated by $z/(1+z)$. If, in any series, $z$ is replaced by $z^2$, then the generated sequence has its members interleaved with 0, for example, $z^2/(1+z^2)$ generates the sequence $\{0,0,1,0,-1,0,1,\ldots\}$. The partial sums of ever more elongated versions of this sequence consist of repeating blocks of "$2^m$ zeros, followed by $2^m$ ones", and the identity holds because any $m$th bit of $n$ is changed by subtraction of $2^m$ from $n$. □

**Lemma 2.** *For integer $m \geq 0$,*

$$\frac{1}{1-z} \cdot \frac{z^{2^{m+1}}}{1+z^{2^m}} \quad \overset{\text{ogf}}{\longleftrightarrow} \quad \{b_{m,n} = [\, m\text{-th bit of } n \text{ exists and is not set}\,]\}. \tag{1.4}$$

*Proof.* The two sequences $a_{m,n}$ and $b_{m,n}$ are **not** the negation of each other, because for example

$$[\,\text{6th bit of 2 exists and is set}\,] = [\,\text{6th bit of 2 exists and is not set}\,] = 0.$$

Since $b_{m,n}$ is not $1 - a_{m,n}$, we cannot simply subtract the g.f. of $a_{m,n}$ from $1/(1-x)$ to get the g.f. of $b_{n,m}$. Rather, the $m$th bit of $n$ does not exist or is unset if the $m$th bit of $n + 2^m$ is set, because the $m$th bit is changed by subtraction of $2^m$. Thus, $b_{m,n}$ is $a_{m,n}$ shifted right by $2^m$ places (the empty placeholders filled with 0), and the g.f. of $b_{m,n}$ is the g.f. of $a_{m,n}$ multiplied with $z^{2^m}$. □

Now, we will compute the recurrence backwards, let $q = \lfloor \log_2 n \rfloor$ the index of the most significant bit, and $p_m = da_{q-m,n} + cb_{q-m,n}$, then

$$\begin{aligned} e(\alpha, c, d; n) &= ((p_0\alpha + p_1)\alpha + p_2)\,\alpha + \cdots \\ &= \alpha^q p_0 + \alpha^{q-1} p_1 + \cdots + \alpha^0 p_q, \\ &= \alpha^q (da_{q,n} + cb_{q,n}) + \alpha^{q-1}(da_{q-1,n} + cb_{q-1,n}) + \cdots + (da_{0,n} + cb_{0,n}). \qquad (1.5) \end{aligned}$$

Using Lemmas 1 and 2, equation (0.2) follows.

**Corollary 1.**

$$e(\alpha, c, d; n) = e(\alpha, c, 0; n) + e(\alpha, 0, d; n) = ce(\alpha, 1, 0; n) + de(\alpha, 0, 1; n). \tag{1.6}$$

$$e(\alpha, 1, 1; n) = \sum_{k=0}^{\lfloor \log_2 n \rfloor} \alpha^k = \begin{cases} \lfloor \log_2 n \rfloor + 1, & \alpha = 1, \\ \dfrac{\alpha^{\lfloor \log_2 n \rfloor + 1} - 1}{\alpha - 1}, & \textit{else}. \end{cases} \tag{1.7}$$

$$e(\alpha, c, d; n) = \begin{cases} (d-c) \cdot e_1(n) \; + \; c(\lfloor \log_2 n \rfloor + 1), & \alpha = 1, \\ (d-c) \cdot e(\alpha, 0, 1; n) \; + \; \dfrac{c\,(\alpha^{\lfloor \log_2 n \rfloor + 1} - 1)}{\alpha - 1}, & \textit{else}. \end{cases} \tag{1.8}$$

*Proof.* Equation (1.6) follows from the main g.f., in (1.7) the main g.f. simplifies by cancelling $(1 + z^{2^k})$ from the fraction, and (1.8) is a consequence of all previous results. □

Identity (1.8) demonstrates that asymptotic behaviour of all sequences discussed in this section is a simple function of the set of "core" sequences $e(\alpha, 0, 1; n)$, the possible descriptions of which (modulo $\alpha$) follow from (1.5):

- Replace $2^k$ with $\alpha^k$ in binary expansion of $n$.
- Sums of distinct powers of $\alpha$.
- $\alpha$-ary representation contains only 0, 1.

Finally, equation (0.3) is a matter of substituting these definitions into eq. (1.8).

## 2. ALTERNATIVE PROOF OF (0.2)

To restate a proposition of us published in the WWW[S2],

**Lemma 3.** *Let $A(z)$ an infinite sum of rational functions of form*

$$A(z) \quad = \quad \sum_{k\geq 0} \alpha^k B(z^{2^k}), \qquad B \text{ rational}, |\alpha| \text{ integer} > 0,$$

*then $A(z)$ generates an integer sequence of divide-and-conquer type satisfying*

$$a_0 = 0, \quad a_{2n} = \alpha \cdot a_n + b_{2n}, \quad a_{2n+1} = b_{2n+1},$$

*where $b_n$ is the sequence generated by $B(z)$.*

Note that the summation term with $k = 0$ fills both bisections of $a_n$ since $\alpha^k$ and $2^k$ reduce to 1. Any other term contributes only to $a_{2n}$ as all exponents to $z$ are even. Moreover, other sequences from single terms of the sum are increasingly sparse (spread out by a factor of 2) and have values multiplied with $\alpha$, with respect to each other. This is essentially the reason for the sequences' fractality.

Using Lemma 3, it is easy to show that

$$\sum_{k\geq 0} \frac{\alpha^k (d \cdot z^{2^k} + c \cdot z^{2^{k+1}})}{1 + z^{2^k}} \quad \overset{\text{ogf}}{\longleftrightarrow} \quad \begin{cases} a_{2n} & = \quad \alpha a_n + c - d, \\ a_{2n+1} & = \quad d - c. \end{cases} \tag{2.1}$$

Let $e'(\alpha, c, d; n)$ the first differences of the sequences $e$ as defined in (0.1):

$$e'(\alpha, c, d; n) \quad = \quad e(\alpha, c, d; n) - e(\alpha, c, d; n-1).$$

We have the four cases

$$\begin{aligned}
e'(4n+1) &= e(4n+1) - e(4n) = \alpha e(2n) + d - \alpha e(2n) - c = d - c \\
e'(4n+2) &= e(4n+2) - e(4n+1) = \alpha e(2n+1) + c - \alpha e(2n) - d \\
&= \alpha(e(2n+1) - e(2n)) + c - d = \alpha e'(2n+1) + c - d \\
e'(4n+3) &= e(4n+3) - e(4n+2) = \alpha e(2n+1) + d - \alpha e(2n+1) - c = d - c \\
e'(4n+4) &= e(4n+4) - e(4n+3) = \alpha e(2n+2) + c - \alpha e(2n+1) - d \\
&= \alpha(e(2n+2) - e(2n+1)) + c - d = \alpha e'(2n+2) + c - d
\end{aligned}$$

The fact[GKP, W] that $(1-z)A(z)$ generates the first differences of $a_n$, together with (2.1) proves the assertion.

We hope that Lemma 3 will help with other proofs of generating functions of this type.

## REFERENCES


[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, 1994

[OEIS] N. J. A. Sloane, editor (2003), *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`

[S1] R. Stephan, *Divide-and-conquer generating functions. I. Elementary sequences*, `math.CO/0307027`

[S2] R. Stephan, *Some divide-and-conquer sequences with (relatively) simple generating functions*, `http://www.research.att.com/~njas/sequences/somedcgf.html` `http://www.ark.in-berlin.de/some2regular.html`

[W] H. S. Wilf, Generatingfunctionology, Academic Press, NY, 1990. `http://www.math.upenn.edu/~wilf/DownldGF.html`