

NOTE

A Pentagonal Number Sieve

Sylvie Corteel* and Carla D. Savage†

*Department of Computer Science, North Carolina State University,
Raleigh, North Carolina 27695-8206*

Herbert S. Wilf‡

*Department of Mathematics, University of Pennsylvania,
Philadelphia, Pennsylvania 19104-6395*

and

Doron Zeilberger§

Department of Mathematics, Temple University, Philadelphia, Pennsylvania

Communicated by George Andrews

Received August 18, 1997

We prove a general “pentagonal sieve” theorem that has corollaries such as the following. First, the number of pairs of partitions of n that have no parts in common is

$$p(n)^2 - p(n-1)^2 - p(n-2)^2 + p(n-5)^2 + p(n-7)^2 - \dots$$

Second, if two unlabeled rooted forests of the same number of vertices are chosen i.u.a.r., then the probability that they have no common tree is .8705.... Third, if f, g are two monic polynomials of the same degree over the field $GF(q)$, then the probability that f, g are relatively prime is $1 - 1/q$. We give explicit involutions for the pentagonal sieve theorem, generalizing earlier mappings found by Bressoud and Zeilberger. © 1998 Academic Press

* Supported in part by NSF grant DMS9302505.

† Supported in part by NSF grant DMS9622772.

‡ Supported in part by the Office of Naval Research.

§ Supported in part by the National Science Foundation.

1. THE MAIN THEOREM

The natural context in which our results lie is that of *prefabs*. A prefab ($[1, 3, 4]$) \mathcal{P} is a combinatorial structure in which each object ω is uniquely representable as a product (“synthesis”) of powers of prime objects, and in which there is an *order* function $\omega \rightarrow |\omega| \in \mathbf{Z}^+$ which satisfies $|\omega\omega'| = |\omega| + |\omega'|$. We denote the primes of \mathcal{P} by p_1, p_2, \dots . Examples of prefabs are integer partitions, rooted unlabeled forests, plane partitions, etc.

Let \mathcal{P} be a prefab in which the number of objects of order n is $f(n)$, for $n = 0, 1, 2, \dots$, and the number of “prime” objects of order n is b_n , for $n \geq 1$. The unique factorization of all objects in \mathcal{P} into products of powers of prime objects is expressed by the formula

$$\sum_{n \geq 0} f(n) x^n = \prod_{i \geq 1} \frac{1}{(1 - x^i)^{b_i}}. \quad (1)$$

For a fixed positive integer m , we are interested here in the number $f_m(n)$, of m -tuples of objects of order n in \mathcal{P} , such that no prime object is a factor of every member of the m -tuple. We will call such a tuple *coprime*. As special cases we mention the number of pairs of partitions of n with no common part, the number of pairs of rooted forests with no common tree, and the number of relatively prime pairs of monic polynomials over a finite field.

To find $f_m(n)$ we note that we can uniquely factor an m -tuple $(\omega_1, \dots, \omega_m)$ of objects of order n into a product of their “gcd” α and an m -tuple $(\omega'_1, \dots, \omega'_m)$ of coprime objects of orders $n - |\alpha|$. Thus

$$\sum_{n \geq 0} f(n)^m x^n = \frac{1}{\prod_{i \geq 1} (1 - x^i)^{b_i}} \sum_{n \geq 0} f_m(n) x^n,$$

which yields

$$\sum_{n \geq 0} f_m(n) x^n = \left(\sum_{n \geq 0} f(n)^m x^n \right) \left(\prod_{i \geq 1} (1 - x^i)^{b_i} \right). \quad (2)$$

This is the general form of the pentagonal number sieve. The effect of multiplying by the product on the right is to sieve out of the generating function for *all* m -tuples of objects of order n , the gf for just the coprime tuples.

Some consequences of the sieve (2) are as follows.

(A) In the prefab of integer partitions, (2) yields the following.

PROPOSITION 1. *The number of m -tuples of partitions of n that have no part in common is*

$$p(n)^m - p(n-1)^m - p(n-2)^m + p(n-5)^m \\ + p(n-7)^m - p(n-12)^m - p(n-15)^m + \dots, \quad (3)$$

in which the decrements are the pentagonal numbers $\{j(3j \pm 1)/2\}_{j \geq 0}$.

(B) Let \mathcal{P} be the prefab of rooted, unlabeled forests. For fixed n , the probability that if we choose two forests of n vertices i.u.a.r. then they will have no tree in common, is, according to (2) with $m=2$,

$$1 + c_1 \left(\frac{f(n-1)}{f(n)} \right)^2 + c_2 \left(\frac{f(n-2)}{f(n)} \right)^2 + \dots,$$

in which $\prod_{i \geq 1} (1 - x^i)^{b_i} = \sum_i c_i x^i$ defines the c 's. Now it is well known that the number of rooted forests of n vertices is $f(n) \sim KC^n/n^{1.5}$, where $C = 2.95576\dots$. Hence each $(f(n-k)/f(n))^2$ above approaches C^{-2k} , and in the limit as $n \rightarrow \infty$ we obtain the following.¹

PROPOSITION 2. *The probability that two rooted forests of n vertices have no tree in common approaches*

$$1 + \frac{c_1}{C^2} + \frac{c_2}{C^4} + \dots = \prod_{i \geq 1} \left(1 - \frac{1}{C^2} \right)^{b_i} = 0.8705\dots$$

as $n \rightarrow \infty$.

(C) Now let \mathcal{P} be the prefab of monic polynomials over a finite field $GF(q)$. There are q^n such polynomials of order (degree) n , so (1) reads as

$$\frac{1}{1 - qx} = \prod_{i \geq 1} \frac{1}{(1 - x^i)^{b_i}},$$

where b_i is the number of irreducible monic polynomials of degree i . Now from (2) we find that

$$\sum_{n \geq 0} f_m(n) x^n = \left(\sum_{n \geq 0} q^{mn} x^n \right) \left(\prod_{i \geq 1} (1 - x^i)^{b_i} \right) = \frac{1 - qx}{1 - q^m x}.$$

If we compare the coefficients of like powers of x on both sides, we find the following.

PROPOSITION 3. *The number of coprime m -tuples of monic polynomials of degree n over $GF(q)$ is $q^{nm} - q^{(n-1)m+1}$. Alternatively, if m monic polynomials*

¹ Dr. Don Zagier observes that this proposition remains true even if the polynomials are (nonconstant and) of different degrees.

of degree n over $GF(q)$ are chosen i.u.a.r., then the probability that their gcd is 1 is $1 - 1/q^{m-1}$.

(D) What is the *average* number of different parts that m randomly chosen partitions of the integer n have in common? We use a well known property of the sieve method: the average number of properties that objects have is $\sum N(\supseteq i)/N$, where i runs over all single properties, $N(\supseteq \{i\})$ is the number of objects that have at least the i th property, and N is the total number of objects. In the present case, the average number of common parts is

$$\frac{1}{p(n)} (p(n-1)^m + p(n-2)^m + \dots + p(1)^m + 1).$$

If we now use the classical asymptotic formula for $p(n)$ it is easy to see that this last expression is $\sim \sqrt{6n}/(m\pi)$. It is well known that the average number of distinct parts in a single random partition of n is $\sim \sqrt{6n}/\pi$. It follows that *the average number of different parts that are common to all members of an m -tuple of partitions of n is $1/m$ th of the average number of distinct parts in a single partition.* For instance, the average number of different common parts in a random pair of partitions of n is one-half of the average number of distinct parts in a single partition of n .

A Question. A special case of Proposition 3 is this: Among the ordered pairs of monic polynomials of degree n over $GF(2)$ there are as many relatively prime pairs as non-relatively prime pairs. What is a nice simple bijection that proves this result?

2. COMBINATORIAL PROOFS

We give combinatorial proofs of (2) and (3) from Section 1.

We rewrite (2) as

$$f_m(n) = \sum_{k \geq 0} f(n-k)^m (q_e(k) - q_o(k)), \quad (4)$$

where $q_e(k)$ (resp. $q_o(k)$) is the number of objects of order k which consist of an even (resp. odd) number of distinct primes. We claim that *any* parity-changing involution which establishes this equation in the $m = 1$ case,

$$\delta_{n,0} = \sum_{k \geq 0} f(n-k)(q_e(k) - q_o(k)), \quad (5)$$

will generalize to an involution for the $m > 1$ case.

To see this, let $F(n)^m, F_m(n)$ be the sets counted by $f(n)^m, f_m(n)$, respectively. For an object α and for $\Omega = (\omega_1, \omega_2, \dots, \omega_m) \in F(n)^m$, let $\alpha\Omega$ denote the m -tuple $(\alpha\omega_1, \alpha\omega_2, \dots, \alpha\omega_m) \in F(n + |\alpha|)^m$. Then any $\Omega \in F(n)^m$ can be decomposed uniquely as $\alpha\Omega'$ for some object α and some $\Omega' \in F_m(n - |\alpha|)$. Thus

$$f(n)^m = \sum_{l \geq 0} f_m(n-l) \cdot f(l). \quad (6)$$

Then using (6) followed by (5) we find

$$\begin{aligned} \sum_{k \geq 0} f(n-k)^m (q_e(k) - q_o(k)) &= \sum_{k, l \geq 0} f_m(n-k-l) \cdot f(l) \cdot (q_e(k) - q_o(k)) \\ &= \sum_{j \geq 0} f_m(n-j) \sum_{k \geq 0} f(j-k) \cdot (q_e(k) - q_o(k)) \\ &= \sum_{j \geq 0} f_m(n-j) \cdot \delta_{j,0} = f_m(n). \end{aligned} \quad (7)$$

Let $Q_e(k), Q_o(k)$ be the sets of objects counted by $q_e(k), q_o(k)$, respectively. Now, suppose we have an involution proof of (5). Specifically, let

$$\psi_1: \bigcup_{k \geq 0} F(n-k) \times F(k) \rightarrow \bigcup_{k \geq 0} F(n-k) \times F(k)$$

be an involution satisfying (i) $\psi_1(\alpha, \beta) = (\alpha, \beta)$ if and only if $\alpha\beta = \lambda$, the empty object (i.e. $n=0$) and otherwise (ii) if $\psi_1(\alpha, \beta) = (\gamma, \delta)$ then $\beta \in Q_e(k)$ if and only if $\delta \in Q_o(k)$.

Then it follows from (7) that for any $m > 1$, ψ_1 extends to the following parity-changing involution ψ_m on $\bigcup_{k \geq 0} (F(n-k)^m \times F(k))$, in which the fixed points are $F_m(n) \times \{\lambda\}$. For $\Omega \in F(n-k)^m$ and $\beta \in F(k)$, decompose Ω as $\alpha\Omega'$, where $\Omega' \in F_m(n-k-|\alpha|)$. Then ψ_m is defined by

$$\psi_m((\Omega, \beta)) = \psi_m((\alpha\Omega', \beta)) = (\gamma\Omega', \delta),$$

where $(\gamma, \delta) = \psi_1((\alpha, \beta))$, thus establishing (4).

Some examples follow.

- The involution of [5] for the inclusion-exclusion principle, adapted for (5) gives the following involution, ψ_m , to prove (2). Let $(\Omega, \beta) \in F(n-k)^m \times F(k)$. Decompose Ω as $\alpha\Omega'$, where $\Omega' \in F_m(n-k-|\alpha|)$ and let

p be the prime factor of largest index, in some fixed list p_1, p_2, \dots of all primes in the prefab, occurring in $\alpha\beta$. Then ψ_m is defined by

$$\psi_m((\Omega, \beta)) = \psi_m((\alpha\Omega', \beta)) = \begin{cases} (\Omega, \beta) & \text{if } \alpha\beta = \lambda \\ (\alpha p\Omega', \beta - p) & \text{if } p \in \beta \\ ((\alpha - p)\Omega', \beta p) & \text{otherwise,} \end{cases}$$

where $\alpha - p$ denotes the object obtained from α by removing one copy of p , and similarly for $\beta - p$.

• In the prefab of integer partitions, we will write a partition of n as a nonincreasing sequence of positive integers $\pi(1) \geq \pi(2) \geq \dots \geq \pi(t) > 0$ such that $|\pi| = \pi(1) + \pi(2) + \dots + \pi(t) = n$. The set of partitions of n is denoted by $P(n)$, its cardinality by $p(n)$. Euler's identity for $p(n)$, $n \geq 1$,

$$\sum_{j \text{ even}} p(n - a(j)) = \sum_{j \text{ odd}} p(n - a(j)),$$

where the $a(j) = (3j^2 + j)/2$ are the pentagonal numbers, and j ranges over all integers, was proved in [2] by exhibiting a bijection between the sets $S_o = \bigcup_{j \text{ odd}} P(n - a(j))$ and $S_e = \bigcup_{j \text{ even}} P(n - a(j))$ for $n > 0$. The bijection can be interpreted as a parity-changing involution Φ_1 on $S_e \cup S_o$, where when $n = 0$, $\Phi_1(\lambda) = \lambda$. This gives a proof of (5), where first Euler's pentagonal number theorem is applied in (5) to replace $q_e(k) - q_o(k)$ by $(-1)^j$ if $k = (3j^2 \pm j)/2$ and by 0 otherwise. Thus, Φ_1 extends to a parity-changing involution, Φ_m on

$$\bigcup_{j \text{ even}} P(n - a(j))^m \cup \bigcup_{j \text{ odd}} P(n - a(j))^m,$$

to prove (3). The involution Φ_m is defined as follows. For $\Pi = \alpha\Pi' \in P(n - a(j))^m$, where $\alpha = (\alpha(1), \dots, \alpha(t))$ and $\Pi' \in P_m(n - |\alpha|)$,

$$\Phi_m(\Pi) = \Phi_m(\alpha\Pi') = \begin{cases} \Pi, & \text{if } j = 0 \quad \text{and} \quad |\alpha| = 0 \\ (t + 3j - 1, \alpha(1) - 1, \dots, \alpha(t) - 1) \Pi', & \\ & \text{if } t + 3j \geq \alpha(1), \\ (\alpha(2) + 1, \dots, \alpha(t) + 1, 1, \dots, 1) \Pi', & \text{where} \\ & \text{there are } (\pi(1) - 3j - t - 1) \text{ ones at the end,} \\ & \text{otherwise.} \end{cases}$$

As a further check, note that $\Phi_m(\Pi) = \Pi$ if and only if $\Pi \in P_m(n)$. Otherwise, $\Pi \in P_e(n)$ if and only if $\Phi_m(\Pi) \in P_o(n)$, where $P_e(n) = \bigcup_{j \text{ even}} P(n - a(j))^m$ and $P_o(n) = \bigcup_{j \text{ odd}} P(n - a(j))^m$. It can be checked that Φ_m is its own inverse.

REFERENCES

1. E. A. Bender and J. R. Goldman, Enumerative uses of generating functions, *Indiana Univ. Math. J.* **20** (1971), 753–765.
2. D. M. Bressoud and D. Zeilberger, Bijecting Euler's partitions-recurrence, *Amer. Math. Monthly* **92**, No. 1 (1985) 54–55.
3. D. Foata and M. Schützenberger, “Théorie géométrique des polynomes euleriens,” Lecture Notes in Math., Vol. 138, Springer-Verlag, Berlin/New York, 1970.
4. A. Nijenhuis and H. S. Wilf, “Combinatorial Algorithms,” 2nd ed., Academic Press, New York, 1978.
5. D. Zeilberger, Garsia and Milne's bijective proof of the inclusion-exclusion principle, *Discrete Math.* **51**, No. 1 (1984) 109–110.