The Lapidary Numbers; or the Combinatorics of Communication by Throwing Stones

Peter Taylor

Preprint (long form) 2014-11-29

Definition

Two spies (Alice and Bob) need to exchange messages. Each will encode their message as a number from 1 to m before they meet. They will then meet by the river and communicate secretly by throwing stones.

There will be a pile of n indistinguishable stones at their meeting point. Starting with Alice, they take turns throwing some of the stones into the river. Each spy must throw at least one stone on their turn, until all n stones are gone.

They observe all throws and separate when there are no more stones. No information is exchanged except the number of stones thrown on each turn.

Given that n is known in advance, what is the largest possible value of m?

Let us call this value the nth lapidary number, from the Latin *lapis, lapidis* meaning *stone*, and denote it $L(n)$. The earliest form of this question of which the author is aware is a February 2011 question on a Russian puzzle site asking whether $L(26) \geq 1700$ [4].

Analysis: decision trees

When there are k stones remaining, the current player can throw 1 to k stones, so the full decision tree for the exchange can be defined inductively. If F_k is the full decision tree when k stones remain, we have that F_{k+1} is a node with $k+1$ children, being one instance of F_i for $0 \leq i \leq k$. (F_0 is a leaf, because there are no stones left to throw).

However, if Alice has the option of throwing all k stones then Bob might not get a chance to throw any, and hence cannot be certain of communicating any more than 1 distinct message. To allow both players to communicate as many messages as possible, they must agree to prune the full tree. Let T_k

be the set of permissible decision trees with k stones remaining, and ε be a placeholder to replace a subtree which has been pruned away. Then we have $T_0 = \{F_0\}$ and

$$T_{k+1} = \left(\prod_{i=0}^{k} T_i \cup \{\varepsilon\} \right) \setminus \prod_{i=0}^{k} \{\varepsilon\}$$

since we can't prune all the subtrees of a node away, as that would leave some stones unthrown.

There is a computationally useful bijection (or identity, if we formalise tuples as nested ordered pairs) which expresses T_{k+1} in terms solely of T_k:

$$\begin{aligned}
T_{k+1} &\equiv \left((T_k \cup \{\varepsilon\}) \times \prod_{i=0}^{k-1} T_i \cup \{\varepsilon\} \right) \setminus \prod_{i=0}^{k} \{\varepsilon\} \\
&= \left(T_k \times \left(T_k \cup \prod_{i=0}^{k-1} \{\varepsilon\} \right) \right) \cup \left(\{\varepsilon\} \times \left(T_k \cup \prod_{i=0}^{k-1} \{\varepsilon\} \right) \right) \setminus \prod_{i=0}^{k} \{\varepsilon\} \\
&= (T_k \times T_k) \cup \left(T_k \times \prod_{i=0}^{k-1} \{\varepsilon\} \right) \cup (\{\varepsilon\} \times T_k)
\end{aligned}$$

We can assign a value to each element $t_k \in T_k$ of (x, y) where $\pi_1(x, y) = x$ is the number of messages which the first player can communicate, and $\pi_2(x, y) = y$ is the number which the second player can communicate. The value of F_0 is $(1, 1)$. For a tree with k stones remaining, $t_k = (t_0, t_1, \ldots, t_{k-1})$, the first player will throw one or more stones to choose one of the children, and will be the second player at that child; so $\pi_1 t_k = \sum_{i=0}^{k-1} \pi_2 t_i$. The second player has no influence over which of the children will be chosen, so $\pi_2 t_k = \min_{i=0}^{k-1} \pi_1 t_i$. This is consistent with the use of ε for pruned subtrees if we assign to ε the value $(0, \infty)$.

If we identify the elements of T_k with their values then the bijection above gives

$$\begin{aligned}
T_{k+1} = \{(x + y, \min(w, z)) \mid (w, x) \in T_k, (y, z) \in T_k\} \\
\cup\, T_k \cup \{(x, w) \mid (w, x) \in T_k\} \quad (1)
\end{aligned}$$

Iterated integer partition sum construction

An *integer partition* λ is a non-increasing sequence of positive integers $(\lambda_1, \lambda_2, \ldots, \lambda_r)$. These integers are called the *parts* of λ. It is sometimes convenient to use the frequency representation $\lambda = (1^{a_1} 2^{a_2} \ldots)$ where a_n is the number of parts which are equal to n. It is also sometimes convenient to represent a partition as a *Ferrers diagram*: a pattern of dots in which the nth row has λ_n dots. The *conjugate* partition λ^* is obtained by transposing the Ferrers diagram of λ.

Let us define the sum of two partitions $\lambda = (1^{a_1} 2^{a_2} \ldots)$ and $\mu = (1^{b_1} 2^{b_2} \ldots)$ as $\lambda + \mu = (1^{a_1+b_1} 2^{a_2+b_2} \ldots)$. This does not appear to be a construction which has been much studied[1], but it allows us to make a surprising connection between the pruned decision trees and integer partitions.

Observe that if $(x, y) \in T_k$ and $x > 1$ then $(x-1, y) \in T_k$ and similarly if $y > 1$ then $(x, y-1) \in T_k$; this must be so, because each spy can deliberately choose not to communicate their highest numbered message, effectively pruning the decision tree. Therefore if we mark the pairs (x, y) on a Cartesian grid we obtain a Ferrers diagram, and hence we obtain a correspondence between T_k and the integer partition whose nth part is $\max\{y \mid (n, y) \in T_k\}$. Moreover, this gives a simpler method of constructing T_k.

Lemma 1. *Define a sequence of integer partitions $\lambda^{(k)}$ iteratively as $\lambda^{(1)} = (1)$ and $\lambda^{(k+1)} = \lambda^{(k)} + \lambda^{(k)*}$. Then T_k corresponds to $\lambda^{(k)}$.*

Proof. By induction. The base case is simple: $T_1 = \{(1, 1)\}$ because there are no decisions to make, and $\lambda^{(1)} = (1)$ by construction.

For the inductive step, the inductive hypothesis combined with equation 1 make it necessary and sufficient to show that

$$\lambda_n^{(k+1)} = \max\left(\left\{\min\left(\lambda_a^{(k)}, \lambda_{n-a}^{(k)*}\right) \middle| 1 \le a < n\right\} \cup \left\{\lambda_n^{(k)}, \lambda_n^{(k)*}\right\}\right) \qquad (2)$$

But this follows almost directly from the sum construction. There exists a such that the first n parts of $\lambda^{(k+1)}$ are the first a parts of $\lambda^{(k)}$ and the first $n - a$ parts of $\lambda^{(k)*}$. If $a = 0$ then $\lambda_n^{(k+1)} = \lambda_n^{(k)*}$; if $a = n$ then $\lambda_n^{(k+1)} = \lambda_n^{(k)}$; and otherwise it is the least of $\lambda_a^{(k)}$ or $\lambda_{n-a}^{(k)*}$ because the parts are non-increasing. Moreover, precisely because the parts are non-decreasing it must be the greatest of the values that would be obtained by taking $a \in \{0, \ldots, n\}$. □

Remark. The sequence $\lambda^{(k)}$ was studied by Naohiro Nomoto in 2002 and he contributed A064660, the sequence of the number of distinct parts in $\lambda^{(k)}$, to the On-Line Encyclopedia of Integer Sequences.[2] Nomoto is unaware of any other publication on the sequence.[2] The author wishes to express his gratitude, as A064660 was the clue which led him to lemma 1.

Remark. It follows from the definition of the lapidary number $L(n)$ and the correspondence between the decision tree T_n and the partition $\lambda^{(n)}$ that $L(n)$

[1] It is not mentioned in the chapter on partitions in Dickson's history[1], nor in Andrews' and Eriksson's more recent overview[3].

[2] Personal correspondence.

is the size of the Durfee square of $\lambda^{(n)}$. By using the frequency representation, this provides the most efficient method known to the author for calculating lapidary numbers. $L(1)$ to $L(60)$ are

1	1	1	2	2	3
4	6	8	12	16	23
31	45	61	87	119	171
233	334	459	655	904	1288
1782	2535	3517	4995	6935	9848
13703	19437	27070	38376	53528	75842
105878	149966	209555	296707	414922	587304
821853	1163052	1628574	2304082	3228091	4566345
6400884	9052798	12695506	17953139	25187813	35614287
49984812	70669026	99219168	140263652	196992898	278461677

Variant construction

Florian Fischer presented without proof an alternative construction.[7] Its correctness follows from the following lemma.

Lemma 2. *Define the pointwise sum of two partitions* λ *and* μ *as* $(\lambda \oplus \mu)_a = \lambda_a + \mu_a$. *Then* $(\lambda + \mu)^* = \lambda^* \oplus \mu^*$.

Proof. The ath part of the conjugate of a partition counts the parts of that partition which are at least a. But by the definition of $\lambda + \mu$, the number of parts which are at least a is the sum of the number of parts in λ and μ which are at least a. □

Corollary 1. *The sequence of partitions* $\lambda^{(k)}$ *can instead be generated as* $\lambda^{(k+1)*} = \lambda^{(k)} \oplus \lambda^{(k)*}$

Proof. By lemma 2 and the definition of lemma 1. □

Partition statistics of $\lambda^{(k)}$

Observation 1. *Nomoto observed that* $\lambda^{(k)}$ *is a partition of* 2^{k-1}.*[2]*

Proof. The sum $\lambda^{(k+1)} = \lambda^{(k)} + \lambda^{(k)*}$ obviously doubles the sum of the parts, and $\lambda^{(1)} = (1)$ is a partition of 2^0. □

Remark. A combinatorial interpretation may be made in terms of the 2^{k-1} possible ways in which the stones other than the first (which must be thrown by Alice) may be thrown.

Observation 2. *Nomoto also pointed out that the largest part* $\lambda_1^{(k)} = F(k)$*, the kth Fibonacci number.*[3] *He must surely have been aware of the closely related property that the number of parts in* $\lambda^{(k)}$ *is* $F(k+1)$*.*

Proof. By induction. For the base case, $\lambda^{(1)} = (1)$ has $F(2) = 1$ parts and the largest part is $F(1) = 1$.

For the inductive step, note that the largest part of λ^* is the number of parts of λ and vice versa. Therefore the number of parts in $\lambda^{(k+1)}$ is $F(k+1)$ from $\lambda^{(k)}$ plus $F(k)$ from $\lambda^{(k)*}$, for a total of $F(k+2)$; and the largest part in $\lambda^{(k+1)}$ is the larger of $F(k)$ from $\lambda^{(k)}$ and $F(k+1)$ from $\lambda^{(k)*}$. ☐

Similar arguments can be used to get expressions for the second-largest part and the number of parts which are equal to 1[4]; for the third-largest part and the number of parts which are equal to 2; etc. Indeed, the author conjectures that for all $n > 1$ there is a monic polynomial $P_n(x)$ of degree $n-3$ such that for $k \geq 3n-4$, $\lambda_n^{(k)} = F(k-1) - \frac{P_n(k)}{(n-3)!}$; and a monic polynomial $Q_n(x)$ of degree $n-1$ such that for $k \geq 3n-1$ the number of parts equal to n is $\frac{Q_n(k)}{(n-1)!}$.

However, this doesn't get us very far towards an expression for the partition statistic which motivated this paper, the Durfee square. Empirically, the lapidary numbers grow exponentially at a rate just under $\sqrt{2}$: i.e. $L(n)$ is just smaller than $2L(n-2)$. A linear growth in the number of largest parts we can accurately evaluate is therefore not sufficient to compute the Durfee square exactly. What we *can* obtain is a loose exponential bound on the Durfee square.

Theorem 1. *The lapidary numbers grow exponentially.*

Proof. That the lapidary numbers cannot grow super-exponentially follows immediately from the fact that $\lambda^{(n)}$ is a partition of 2^{n-1}, and its Durfee square is thus bounded above by $2^{(n-1)/2}$.

Any stone-throwing strategy gives a lower bound. A simple strategy proposed by Joe Zeng[6] gives an exponential lower bound as follows: suppose that we assign a stones to Alice and $b = n - a$ stones to Bob, and that both Alice and Bob guarantee to make t throws. Then Alice actually has the option of making $t+1$ throws. Counting the possible ways they can divide their stones between their throws is a classic stars and bars problem, with the result that Alice can communicate $\binom{a-1}{t-1} + \binom{a-1}{t} = \binom{a}{t}$ distinct values, and Bob can communicate $\binom{b-1}{t-1}$ distinct values, giving a lower bound $L(n) \geq \min\left(\binom{a}{t}, \binom{b-1}{t-1}\right)$.

[3] This is according to the convention that $F(1) = F(2) = 1$.

[4] Respectively $F(k-1)$ and $F(k-1)+1$.

If $n = 4m$ then we set $a = b = 2m$ and $t = m$ to get $L(n) \geq \min\left(\binom{2m}{m}, \binom{2m-1}{m-1}\right) = \binom{2m-1}{m-1} = \left(2 - \frac{1}{m}\right)\binom{2m-2}{m-1} \geq \left(2 - \frac{1}{m}\right)\frac{4^{m-1}}{\sqrt{4(m-1)}} = \left(\frac{1}{2} - \frac{1}{n}\right)\frac{2^{n/2}}{\sqrt{n-4}}$, so $L(n)$ is within a rational polynomial factor of $2^{n/2}$. The precise selection of a and t varies for different values of $n \bmod 4$, but a lower bound for $L(4m)$ is also a loose lower bound for $L(4m + i)$ for fixed i, since the lapidary numbers are non-decreasing. □

Simple modifications of this argument can tighten the lower bound, but only appear to improve the constant factor.[5]

Notes on possible directions for continued investigation

A simple numerical check rules out a recurrence along the lines of $L(n) = \sum_i \sum_j a_{i,j} n^i L(n-j)$ for moderate ranges of i and j, and the OEIS Superseeker does not shed any light on a possible generating function for $L(n)$ or for $L(4n)$.

The only promising link to sequences in OEIS with a similar growth rate is with A064660, the number of distinct parts of λ_n; there seems to be a trend towards A064660$(n) = \alpha L(n)$ where α is about 1.8. Given the already established links to Fibonacci numbers, it does not seem implausible that α should be $\frac{5+\sqrt{5}}{4} = 1 + \frac{\phi}{2}$, but empirically it seems to be trending to a value slightly below that.

References

[1] History of the Theory of Numbers, Vol. II (Diophantine Analysis), L. E. Dickson, Carnegie Institution of Washington (1920).

[5] Consider what happens if a player holds back some stones. Alice may throw all of her stones in t or $t+1$ throws, but if she holds r stones back after $t+1$ throws then they may be used in a sub-game where Bob throws first but only aims to communicate one number; in this case we look at $\lambda_1^{(r)}$ to see that Alice can use those r stones in $F(r)$ ways, so that she has $\binom{a}{t} + \sum_{r=1}^{a-t-1} \binom{a-r-1}{t} F(r)$ options. Similarly Bob has $\binom{b-1}{t-1} + \sum_{r=1}^{b-t} \binom{b-r-1}{t-1} F(r)$ options.

If we again consider $n = 4m$ and choose $a = b = 2m$ and $t = m$ we again find that Bob is the player with fewer options, so that $L(n) \geq \binom{2m-1}{m-1} + \sum_{r=1}^{m} \binom{2m-r-1}{m-1} F(r)$. This additional term can be shown via the main theorem of [5] to have g.f. $\frac{z}{1-4z+z\sqrt{1-4z}} = \frac{1}{\sqrt{1-4z}} - \frac{1}{z+\sqrt{1-4z}}$ so the improvement is less than a factor of 2.

[2] Sequence A064660, The On-Line Encyclopedia of Integer Sequences, published electronically at http://oeis.org/A064660, retrieved 2014-06-16.

[3] Integer Partitions, G. E. Andrews and K. Eriksson, Cambridge University Press (2004).

[4] Обмен шифрами, posted on 2011-02-01 by user tatunya at https://braingames.ru/index.php?path=comments&puzzle=475, retrieved 2014-06-16.

[5] On the Central Coefficients of Riordan Matrices, P. Barry, Journal of Integer Sequences, Vol. 16 (2013)

[6] Two Spies Throwing Stones Into a River, Joe Zeng's answer posted 2014-06-08 at http://puzzling.stackexchange.com/a/630, retrieved 2014-06-08.

[7] Build a pair of spies that will throw stones into a river, Florian Fischer's answer posted 2014-10-05 at http://codegolf.stackexchange.com/a/38560, retrieved 2014-10-05.