On the total sum of number of nodes covering a given number of leaves in an unordered binary tree

Nozomu Ochiumi
Tokyo University of Science

Let J be a subset of leaves in a finite rooted tree T with leaf-set U. If we delete all the paths (and all the edges incident to them) that connect the root and the leaves in $U \setminus J$, then there remains a forest comprising, say, c subtrees of T. We may say that, in the whole tree T, the c nodes, the roots of these subtrees, *cover* or dominate J (and only J), and call c the *covering number* for J.

The "cover" concept for rooted trees seems to be originated in the works [1][6] on a certain cryptographic key-management problem of a broadcast type with $|U|$ users, and the covering number can be considered a new combinatorial topic in the theory of rooted trees. We believe that it is worthwhile to investigate covering numbers from the view point of combinatorics and derive mathematical results such as the distribution and expected value of the covering number for J with respect to a certain probability measure $P(T)$, $T \in \mathcal{T}$, where $\mathcal{T}$ is the set of all binary trees (either ordered or unordered) with n $(= |U|)$ leaves. The main purpose of this paper is to find an explicit formula for the average covering number for J in the case where T is an unordered binary tree with labeled leaves and $P(T)$ is uniform, i.e., $P(T) = |\mathcal{T}|^{-1}$ (see [2] for a corresponding study on the completely balanced binary tree with 2^k leaves).

As is described in [5], an unordered binary tree with n labeled leaves $1, 2, \ldots, n$ is a graphic representation of a "binary total partition" of $U = \{1, 2, \ldots, n\}$; partition U (the root) into two non-empty subsets (unordered two children of the root), similarly bipartition each of these subsets, $\ldots$, continued until we have n singleton sets (n leaves). Denote by $\mathcal{T}_U$ the set of all such binary trees having n leaves and put $b_n = |\mathcal{T}_U|$, then it is shown that $b_1 = 1$ and

$$b_n = \frac{1}{2} \sum_{k=1}^{n-1} \binom{n}{k} b_k b_{n-k}, \ n \geqslant 2,$$

which leads us to the formula $b_n = (2n-3)!!$ (as was originally given in [3]), where $n!!$ means the double-factorial (define $(-1)!! = 1$ and $b_0 = 0$).

Let $c_T(J)$ be the covering number for a subset $J \subset U$ of leaves in a finite rooted tree $T \in \mathcal{T}_U$ and define $c_T(\emptyset) = 0$. We are interested in finding the average covering number for J of size k, defined as $\frac{a_{n,k}}{b_n}$, where

$$a_{n,k} = \sum_{T \in \mathcal{T}_U} c_T(J), \ 0 \leqslant k \leqslant n = |U|, \ J \in \binom{U}{k}.$$

Note that the average covering number is independent of the choice of J, that is,

$$\sum_{T \in \mathcal{T}_U} c_T(J) = \sum_{T \in \mathcal{T}_U} c_T(J'), \ J, J' \in \binom{U}{k}.$$

We derive a recurrence relation for $a_{n,k}$ and give an explicit expression for the average covering number.

Let $a_{n,k} = 0$ $(k > n)$ for convenience sake. It is clear that $a_{n,n} = b_n$ $(n \geqslant 1)$ by the definition of $a_{n,k}$. We first show that $a_{n,k}$'s satisfy the following recursion.

Theorem 1. *For* $1 \leqslant k \leqslant n-1$,

$$\begin{aligned} a_{n,k} &= \sum_{l=1}^{n-1} \sum_{i=1}^{k} \binom{k}{i} \binom{n-k}{l-i} (2(n-l)-3)!! a_{l,i} \\ &= \sum_{i=1}^{k} \sum_{j=0}^{n-k} \binom{k}{i} \binom{n-k}{j} (2(n-i-j)-3)!! a_{i+j,i}. \end{aligned}$$

Next we derive the formula for the general term $a_{n,k}$ by the generating function method.

Theorem 2. *For* $n \geqslant 2$,

$$a_{n,k} = (2(n-k)-1)!! \left(\frac{(2n-2)!!}{(2(n-k)-2)!!} - \frac{(2n-3)!!}{(2(n-k)-3)!!} \right), \ 1 \leqslant k \leqslant n-1.$$

We remark that $a_{n,n-1} = (2n-2)!! - (2n-3)!!$. This special case is mentioned in [4, A129890] without its sources.

References

[1] D. Naor, M. Naor, J. Lotspiech, Revocation and tracing schemes for stateless receivers, Advances in Cryptology—CRYPTO 2001 (Santa Barbara, CA), vol. 2139 of Lecture Notes in Comput. Sci., Springer, Berlin, 2001, pp. 41–62.

[2] E. C. Park, I. F. Blake, On the mean number of encryptions for tree-based broadcast encryption schemes, J. Discrete Algorithms, 4 (2) (2006) 215–238.

[3] E. Schröder, Vier kombinatorische Probleme, Z. für Math. Phys., 15 (1870) 361–376.

[4] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences,
http://www.research.att.com/˜njas/sequences

[5] R. P. Stanley, Enumerative Combinatorics. Vol. 2, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1999.

[6] C. K. Wong, M. G. Gouda, S. S. Lam, Secure group communications using key graphs, IEEE/ACM Trans. Networking, 8 (1) (2000) 16–30.