Prove that it is sufficient to check $\lceil \log(k) \rceil$ pairs to tell if a set of integers is pairwise coprime

I am reading chapter 31 of Introduction to Algorithms (CRLS) and I encountered some difficulties while solving 31.2-9. I managed to prove the first part of a problem, but I can't prove the generalized version.

This is the problem statement:

> Prove that n_1, n_2, n_3, and n_4 are pairwise relatively prime if and only if $gcd(n_1n_2, n_3n_4) = gcd(n_1n_3, n_2n_4) = 1$. More generally, show that $n_1, n_2, \ldots, n_k$ are pairwise relatively prime if and only if a set of $\lceil \log(k) \rceil$ pairs of numbers derived from the n_i are relatively prime.

Proof of the first part: $gcd(n_1n_2, n_3n_4) = 1$ means that n_1n_2 and n_3n_4 doesn't have any common factors, so $gcd(n_1, n_3) = gcd(n_1, n_4) = gcd(n_2, n_3) = gcd(n_2, n_4) = 1$ The same is for the second equation so, $gcd(n_1, n_2) = gcd(n_1, n_4) = gcd(n_3, n_2) = gcd(n_3, n_4) = 1$

(number-theory) (algorithms)

edited May 27 '16 at 18:07

asked May 27 '16 at 17:53
J. Abraham
118 9

Is the log in the ceiling of $\log(k)$ the base 2 log? At least that would give for $k = 4$ the result of 2 sets of numbers as in your example, . – coffeemath May 27 '16 at 18:27

Hint: en.wikipedia.org/wiki/Hadamard_matrix – Jack D'Aurizio May 27 '16 at 18:36

Yes, it is in base 2. – J. Abraham May 27 '16 at 18:40

1 Answer

Hint: Assume that we have k positive integers $a_0, \ldots, a_{k-1}$ and $k \leq 2^m$. For any j such that $1 \leq j \leq m$, we define $f_j(m)$ as the value of the $(j-1)$-th bit from the right in the binary representation of m, then take:

$$N_1^{(j)} = \prod_{k:f_j(k)=1} a_k, \qquad N_0^{(j)} = \prod_{k:f_j(k)=0} a_k$$

and compute $G_j = \gcd\left(N_0^{(j)}, N_1^{(j)}\right)$. If $G_j = 1$ for any j in the range $[1, m]$, the original integers are pairwise coprime, otherwise they are not. And obviously $m \approx \log_2(k)$.

This construction is kindly stolen from Hadamard matrices.

answered May 27 '16 at 18:45
Jack D'Aurizio
189k 17 173 438

How is this related to Hadamard matrices? What parts of the wiki article cited should I read? – hengxin yesterday

@hengxin: indeed a more accurate reference is en.wikipedia.org/wiki/Sperner%27s_theorem – Jack D'Aurizio yesterday

Still confused. Would you please provide more details? What are the characterizations of $N_1^{(j)}$ and $N_0^{(j)}$ and how are they related to the Sperner theorem? It seems that there are some patterns. But I failed to identify them. Thanks. – hengxin yesterday

I found that the problem of covering a (complete) graph by complete bipartite graphs is closely related to this problem. For example, see the paper On covering graphs by complete bipartite subgraphs by S. Jukna and A.S. Kulikov, 2009. – hengxin 15 mins ago edit