

Re: minimum Hamming distance among random bit vectors

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-04/2710.html>

From: Francois Grieru (fgrieru_at_francenet.fr)

Date: 04/29/04

Date: Thu, 29 Apr 2004 22:34:02 +0200

In article <vm6kc.13304\$os1.11938@newssvr31.news.prodigy.com>, Mike Amling wrote:

> *How can there be a nonzero probability of "two distinct vectors which differ by at most" 0 bits?*

Problem comes from my misuse of "set" instead of "array" of vectors, and of "distinct vectors" to refer to vectors in distinct entries.

Formally:

With X_{ij} denoting random unbiased independent bits, $p(b,n,d)$ is the probability that there exists indexes r s such that $0 \leq r < n$, $0 \leq s < n$, $r \neq s$, $d \geq \sum_{j=0}^{b-1} (X_{rj} \text{ xor } X_{sj})$

Or more simply:

$p(b,n,d)$ is the probability that among n random vectors of b bits, there are two which differ by at most d bits.

> > *I also fail to characterise*
> > $N(b,d) = \min(n \text{ such that } p(b,n,d)=1)$
>
> *Of course* $N(b,d) \leq (2^b)/v(b,d)+1$,
> *where* $v(b,d)$ *is the sum for* $k=0$ *through* d *of* $C(b,k)$.

Maybe, but I fail to see why. I'm stuck at the bound suggested by Keith Lewis, which assigns a "ball" of radius $\text{floor}(d/2)$ to each of the n vectors, giving

$$N(b,d) \leq 2^b / v(b, \text{floor}(d/2))$$

Francois Grieru