Combinatorial Structures in Cryptology: Cover-Free Families

December 13, 2006

Let $\mathcal{U}$ be a finite universe, and write $|\mathcal{U}| = n$. A family $\mathcal{F}$ of subsets of $\mathcal{U}$ is independent if for each $U, V \in \mathcal{F}$ with $U \neq V$ it holds that neither $U \subset V$ nor $V \subset U$. In other words, $\mathcal{F}$ is an independent set in the partial order on the powerset $\mathcal{P}(\mathcal{U})$ induced by set-inclusion. $\mathcal{F}$ is maximal independent if there is no independent family $\mathcal{F}'$ that properly contains $\mathcal{F}$. What can you say about the maximum size of an independent family?

It is a classical result in combinatorics that an independent family $\mathcal{F}$ satisfies $|\mathcal{F}| \leq \binom{n}{\frac{n}{2}}$ if n is even and $|\mathcal{F}| \leq \binom{n}{\frac{n-1}{2}}$ if n is odd. In the case where n is even, equality holds if and only if $\mathcal{F}$ consists of all subsets of size $\frac{n}{2}$. In the case where n is odd, equality holds if and only if $\mathcal{F}$ consists of all subsets of size $\frac{n-1}{2}$ or $\mathcal{F}$ consists of all subsets of size $\frac{n+1}{2}$. This was shown by E. Sperner in his article "Ein Satz über Untermengen einer endlichen Menge," which appeared in Matematische Zeitschrift, 27: 544–548 (1928). Independent families are also called Sperner families in the literature.

In the context of their work on error correcting codes, W. H. Kautz and R. C. Singleton generalized the notion of Sperner families as follows. An r-cover-free family $\mathcal{F}$ consists of a finite universe $\mathcal{U}$ together with a collection of non-empty, distinct subsets $V_1, \ldots, V_m \subset \mathcal{U}$ such that for each index $i \in \{1, \ldots, m\}$ and for each set of indices $J \subset \{1, \ldots, m\}$ with $i \notin J$ and $|J| \leq r$ it holds that $V_i \not\subset \cup_{k \in J} V_k$. In other words, no set is covered by the union of r other sets. The case $r = 1$ corresponds to Sperner families. See the article "Nonrandom Binary Superimposed Codes" by Kautz and Singleton in IEEE Transactions in Information Theory, vol. IT-10, pp. 363–377, October 1964.[1]

Let $N(r, m)$ denote the minimum size of a universe $\mathcal{U}$ such that there exists an r-cover free family $\mathcal{F}$ on $\mathcal{U}$ with $|\mathcal{F}| = m$. What is known about this quantity? For instance, it is known that there is a constant c such that $N(r, m) \geq c \frac{r^2}{\log r} \log m$. Upper bounds are known as well.

Cover-free families have numerous application in cryptology (and beyond). We study (efficient) constructions from error codes and algebraic curves, upper- and lower bounds, as well as applications to broadcast encryption, traitor tracing, blacklisting, and bounded CCA secure encryption.

[1] One also considers the more general notion of (w, r)-cover-freeness, which requires that no intersection of w sets is contained in the union of r other sets.