Several months ago there was a problem on Math Magic asking what is the size $C(n,m)$ of a boolean circuit that can determine whether at least m of its n inputs are 1's. No good answers were obtained for that problem until two weeks ago when Sasha Ravsky obtained an upper bound $C(2^n,2) \leq 3n+1$. Since the solution was not published on the website, but only the results, I e-mailed Sasha and asked him what his solution was. When I received his e-mail I realized that his method could be extended to yield an upper bound for $C(n,m)$ for all m. My modification of his argument is below.

The function we want to represent is

$$f(x_1,\ldots,x_n) = \bigvee_{\substack{A\in[1,n]\\|A|=m}} \bigwedge_{i\in A} x_i.$$

We will try to represent this function as

$$f(x_1,\ldots,x_n) = \bigvee_{j=1}^{k} \bigwedge_{i=1}^{m} \bigvee_{r\in D_{j,i}} x_r,$$

where D_j are partitions of the set $[1,n]$ into disjoint sets

$$[1,n] = D_{j,1} \cup D_{j,2} \cup \cdots \cup D_{j,m}, \qquad D_{j,i_1} \cap D_{j,i_2} = \emptyset,$$

which are to be determined later. The necessary and sufficient condition on these partitions for such representation of f to work is that for every m-tuple of numbers in $[1,n]$ there is a partition D_j such that every element of the m-tuple belongs to exactly one of $D_{j,i}$. In this case we'll say that collection $D_{j,i}$ is a separating partition system. Since to represent function f using this scheme it is sufficient to use $1+k(m+1)$ gates, our goal is minimize k, the number of partitions in the partition system.

Sasha Ravsky noted that if $m=2$ then $D_{j,i} = \{r \mid j\text{'th bit of } r \text{ is } i\}$ is a separating partition system. This partition system is optimal since one needs at least $\log_2 n$ bits of information to distinguish two elements in n-element set. The problem of constructing the minimal separating partition system for $m>2$ seems to be much harder, but a good upper bound on number of elements in such system can be easily obtained using the standard probabilistic techniques.

Let's fix some m-tuple of numbers from $[1,n]$, and consider a random partition of the set $[1,n]$ into m sets, where each number can the equal chances of getting into every of these m sets. The probability, that such partition separates the m-tuple in question, is obviously $\frac{m!}{m^m}$. The probability, that neither of k' such random partitions (some of them might be same) separate the m-tuple is $(1-\frac{m!}{m^m})^k$. The expected number of m-tuples which are not separated is therefore $t = \binom{m}{n}(1-\frac{m!}{m^m})^{k'}$, and so there exists at least one partition system consisting of k' partitions such that it does not separate at most t m-tuples. Hence, we can construct a separating partition system consisting of at most

$$t + k' = t - \log_b t + \log_b \binom{m}{n}$$

where $b = \frac{m^m}{m^m - m!}$. Since $\binom{m}{n} < n^m/m!$ and $2 - \log_b 2 - \log_b m! \le 0$ for $m \ge 2$,

$$k \le m \log_b n.$$

Thus we have proved a

Theorem 1 *For $m \ge 2$, $C(n,m) \le 1 + m(m+1)\log_b n$.*