Example 4 On Van Der Waerden's Theorem

Van der Waerden proved that for all $k \geq 1$ there exists W_k such that if $n \geq W_k$ and the integers in $[n]$ are partitioned into $R \cup B$ (2-coloured) then at least one of R, B contains a k-term arithmetic progression i.e. a sequence $a, a+b, a+2b, \ldots, a+(k-1)b$ for some $a, b > 0$.

Theorem 1.

$$W_k \geq 2^{k/2}.$$

Proof Colour $[n]$ randomly. For each S, $|S| = k$, $S = \{i_1 < i_2 < \cdots < i_k\}$ is an arithmetic progression, let A_S be the event "S is mono-coloured". Then

$$\mathbf{Pr}(A_S) = 2^{1-k}.$$

The number of possible S is at most $\binom{n}{2}$ since once we have chosen i_1, i_2 then the remaining elements are determined. So,

$$\mathbf{Pr}(\exists S : \ A_S) \leq \binom{n}{2} 2^{1-k} < n^2 2^k \leq 1.$$

□

Example 5 Key distribution

n people wish to communicate securely. There are ℓ keys, $K = \{k_1, k_2, \ldots, k_\ell\}$ available. Each person i is to be given a set $A_i \subseteq [\ell]$ and the corresponding set of keys $K_i = \{k_j : \ j \in A_i\}$.

The sets $A_1, A_2, \ldots, A_n$ are to be public knowledge, but a person only knows the actual keys associated with the set he is given. If person i wishes to communicate with person j he sends the keys in $K_i \cap K_j$ to j, in order to identify himself. Security is compromised if $\exists k$ such that $A_k \subseteq A_i \cap A_j$, for then k can pretend to be j.

How big does ℓ have to be.

Theorem 2. *There is a scheme if* $\ell \geq \frac{3 \log n}{\log 8/7}$.

Proof Choose $A_1, A_2, \ldots, A_n$ randomly. Let

$$\mathcal{E}_{i,j,k} = \{A_k \supseteq A_i \cap A_j\}.$$

Then

$$\mathbf{Pr}(\mathcal{E}_{i,j,k}) = \left(\frac{7}{8}\right)^\ell.$$

This is because $\mathcal{E}_{i,j,k}$ occurs iff for every $x \in [\ell]$ it is **not** the case that $x \in A_i, x \in A_j$ and $x \notin A_k$.

But then

$$\mathbf{Pr}(\exists i, j, k : \ \mathcal{E}_{i,j,k} \text{ occurs}) \leq 3\binom{n}{3}\left(\frac{7}{8}\right)^\ell < 1.$$

□

Finally note that we must have $2^\ell \geq n$ or $\ell \geq \log_2 n$, for otherwise we cannot give everybody a distinct set. This can be improved slightly. Define $B_{i,j} = A_i \cap A_j$. Then the sets $B_{i,j}$ are a Sperner System i.e. an anti-chain in the power-set of $[\ell]$. The number of $B_{i,j}$ is $\binom{n}{2}$. Thus from Sperner's theorem, we have

$$\binom{n}{2} \leq \binom{\ell}{\lfloor \ell/2 \rfloor}$$

which implies that we need $\ell \geq 2 \log_2 n$.