A Puzzle on Block Design
Jayadev Misra
7/6/06

1 Problem Description

The following puzzle comes from Adam Klivans, who heard it second hand from Peter Winkler. A *secret* is a triple where each component is a natural number below n, for some given n. A *guess* is a triple of the same form. A guess has an outcome which is revealed to the guesser: it succeeds if it matches at least two corresponding components of the secret, and fails otherwise. What is the minimum number of guesses required to succeed for $n = 8$?

We give a schedule of $n^2/2$ guesses for even n and $(n^2 + 1)/2$ for odd n.

2 A Solution Procedure

We solve a simpler problem first. Let V be a set of m values, $m > 0$. Construct a schedule which succeeds if at least two values in the secret are from V. Not all values in the secret are required to be from V, and this is how this problem differs from the original. We show a schedule of length m^2 to solve this problem. We also show that m^2 is a tight bound.

We can solve the original problem using the solution of the simpler problem. Suppose the number of values, n, is even. Divide the n values into two equal-sized sets, U and V. Let S be a schedule for U and T for V, for the simpler problem. We claim that S and T together solve the original problem. Since the secret has three components, at least two of the components are from U or from V. In the former case, S succeeds and in the latter case, T succeeds. Therefore, the combined schedule succeeds in all cases. The length of each of S and T is $(n/2)^2$; so the combined length of both schedules is $n^2/2$. For odd n, say $n = 2m + 1$, let U and V have m and $m + 1$ values, respectively. The same procedure creates a combined schedule of length $m^2 + (m + 1)^2 = ((2m + 1)^2 + 1)/2 = (n^2 + 1)/2$. For $n = 8$, the schedule length is $8^2/2 = 32$.

Solution of the Simpler Problem Given is a set V, $V = \{v_i |\ 0 \leq i < m\}$. Let the schedule consist of all guesses (v_i, v_j, v_k), where $(i + j + k) \bmod m = 0$. To see the correctness, suppose (p, q, r) is the secret. Without loss in generality, let p and q be from V, say $p, q = v_a, v_b$. Let c be such that $(a+b+c) \bmod m = 0$. Such a c exists and is unique. Then, (v_a, v_b, v_c) is a guess in the schedule, and it succeeds. As an example, we list the schedule for $V = \{0, 1, 2, 3\}$, i.e., $v_i = i$.

(0 0 0)	(0 1 3)	(0 2 2)	(0 3 1)
(1 0 3)	(1 1 2)	(1 2 1)	(1 3 0)
(2 0 2)	(2 1 1)	(2 2 0)	(2 3 3)
(3 0 1)	(3 1 0)	(3 2 3)	(3 3 2)

The length of the given schedule is m^2 where m is the size of V. This is because there is a 1-1 correspondence between pairs (i, j), $0 \le i, j < m$, and guesses in the schedule; (i, j) corresponds to the guess (v_i, v_j, v_k), where k is given by $(i + j + k) \bmod m = 0$.

Next, we show that m^2 is a lower bound on the length of any schedule to solve this problem. Otherwise, let there be a shorter schedule s. Let $s' = \{(u, v) | \ (u, v, w) \in s, \text{ for some } w\}$. Since the length if s is less than m^2, so is the length of s'. Therefore, there is a pair (p, q) which is not in s', i.e., $(p, q, r) \notin s$ for any r. Let the secret be (p, q, x), where x is a value outside V. The schedule does not succeed in guessing this secret.

3 Some Observations on Lower Bound

A trivial lower bound is $n^3/(3n - 2)$. This is seen as follows. A triple t *covers* a triple s if they match in at least two components. Therefore, the Hamming distance between the triples is at most 1. Any triple t covers itself (at Hamming distance of 0) and covers at most $3n - 3$ other triples at Hamming distance 1 (by changing each component in $n - 1$ possible ways). For $n = 2$, this gives a lower bound of 2. For $n = 4$, the lower bound is 7, differing from our schedule of length of 8.

It may be possible to get a tighter lower bound using the following lemma. Let S be a schedule. Extract pairs from it as follows.

$$s_{12} = \{(i, j) | \ (i, j, -) \in s\}$$
$$s_{13} = \{(i, k) | \ (i, -, k) \in s\}$$
$$s_{23} = \{(j, k) | \ (-, j, k) \in s\}$$

And,

$$p_i = \{k | \ (i, k) \in s_{13}\}$$
$$q_j = \{k | \ (j, k) \in s_{23}\}$$

Lemma $(i, j) \notin s_{12} \ \Rightarrow \ |p_i| + |q_j| \ge n$
Proof: Suppose $|p_i| + |q_j| < n$. Then $|p_i \cup q_j| \le |p_i| + |q_j| < n$. Therefore, there exists k, where $k \notin p_i \cup q_j$, i.e., $k \notin p_i$ and $k \notin q_j$. That is,

$(i, k) \notin s_{13}$, from $k \notin p_i$
$(j, k) \notin s_{23}$, from $k \notin q_j$
$(i, j) \notin s_{12}$, given

Then, the secret (i, j, k) is not covered by s.