

## Zuckerman's problem and the ETAC

Thanks to David Zuckerman, the following problem circulated, before I left for Europe, at the Department in Austin.

At a University with  $N$  professors, committees have to be formed under the following constraints.

C0: each committee consists of an odd number of professors

C1: any two distinct committees share an even number of professors.

What is the maximum number of committees that can be formed?

\*            \*            \*

Before leaving the USA I had thought about the problem but had not solved it. The  $N$  distinct committees each consisting of a single professor meet both constraints, so the answer is  $\geq N$ . Exploring the possibilities for a few small values of  $N$  gave me the "moral certainty" that the answer was also  $\leq N$ .

I quickly decided not to use set notation, which I don't like (never having found it helpful) but to characterize instead each committee by a vector of  $N$  bits. It took me more time to decide how to interpret these bits: were they

booleans representing true/false, or were they integers representing 0/1.

Initially I was attracted by the boolean interpretation because the continued equivalence expresses so nicely the evenness of the number of its false arguments and C0 requires us to pay attention to such odd/evenness. In C1, however, the notion of sharing requires us to pay attention to the identity of the professors as well, but this identity is not really reflected in the continued equivalence which is defined on unordered bags of arguments. Thus I found that in the context of this problem I could not manipulate the continued equivalence in a meaningful manner.

Turning my attention to the integer interpretation I realized that both constraints could be expressed without explicit mention of the individual professors in terms of the scalar product.

Note The scalar product  $\cdot$  is defined on pairs of integer sequences of equal length by

$$[] \cdot [] = 0$$

$$[x:xs] \cdot [y:yz] = x \cdot y + [xs] \cdot [ys] \quad (\text{End of Note})$$

Here is the problem as I posed it to the ETAC

on Tuesday 12 June 2001.

Consider a set  $V$  of 0/1 vectors of  $N$  components such that

$$C_0: \langle \forall i: v_i \in V: \text{odd.}(v_i \cdot v_i) \rangle$$

$$C_1: \langle \forall i, j: v_i, v_j \in V \wedge i \neq j: \text{even.}(v_i \cdot v_j) \rangle$$

Show that  $V$  contains at most  $N$  vectors.

Remark The two constraints can elegantly be combined into

$$\langle \forall i, j: v_i, v_j \in V: i=j \equiv \text{odd.}(v_i \cdot v_j) \rangle$$

and this is very encouraging. (End of Remark)

Because in  $N$ -dimensional space there are no sets of more than  $N$  linearly independent vectors, the ETAC set out to solve the problem by showing that the vectors in  $V$  are linearly independent. Let  $O_N$  denote the zero-vector of length  $N$  and let  $\alpha$  be a sequence of as many coefficients as there are vectors in  $V$ . Linear independence of the vectors  $v_i$  in  $V$  then means that for any  $\alpha$

$$(0) \quad \langle \sum_i: \alpha_i \cdot v_i \rangle = O_N \Rightarrow \langle \forall i: \alpha_i = 0 \rangle$$

In my experience with linear algebra, the components of the vectors and the coefficients  $\alpha_i$  of the linear composition used to range over the real numbers, but fortunately some of the ETAC members knew that the whole

theory is also applicable in the field of rational numbers. The vector components being integer, and hence rational, it suffices to prove (0) for rational  $\alpha$ . But since left- and right-hand side of (0) are invariant for multiplication of  $\alpha$  by a constant that differs from zero, we can confine our attention to integer  $\alpha$ . (Because the number of  $v_i$  is at most  $2^N$ , i.e. finite, we can multiply  $\alpha$  by a common multiple of the denominators of the  $\alpha_i$  to get all coefficients integer.) From now on,  $\alpha$  stands for a sequence of integer coefficients. We observe for any  $j$  in range

$$\langle \sum_{i::} \alpha_i \cdot v_i \rangle = 0_N$$

$$\Rightarrow \{ 0_N \cdot v_j = 0 \}$$

$$\langle \sum_{i::} \alpha_i \cdot v_i \rangle \cdot v_j = 0$$

$$\equiv \{ \cdot \text{ distributes over } \Sigma \}$$

$$\langle \sum_{i::} (\alpha_i \cdot v_i) \cdot v_j \rangle = 0$$

$$\equiv \{ \cdot \text{ and } \cdot \text{ mutually associative} \}$$

$$\langle \sum_{i::} \alpha_i \cdot (v_i \cdot v_j) \rangle = 0$$

$$\equiv \{ \text{split range; 1-point rule} \}$$

$$\langle \sum_{i::} i \neq j: \alpha_i \cdot (v_i \cdot v_j) \rangle + \alpha_j \cdot (v_j \cdot v_j) = 0$$

$\Rightarrow \{ \alpha_i \text{ integer; } C1, \text{ i.e. even. } (v_i \cdot v_j) \}$

even.  $(\alpha_j \cdot (v_j \cdot v_j))$

$\Rightarrow \{ C0, \text{ i.e. odd. } (v_j \cdot v_j) \}$

even.  $\alpha_j$

The above calculation implies with the aid of some elementary algebra that  
 (1)  $\text{int. } \alpha \wedge \langle \sum_i \alpha_i \cdot v_i \rangle = 0_N$   
 is invariant under  $\alpha := \alpha/2$ , which allows us to conclude that under the truth of (1), each  $\alpha_j$  is divisible by arbitrarily high powers of 2 and hence  $= 0$ . And thus, (0) has been established.

Nuenen, 25 June 2001

prof. dr Edsger W. Dijkstra  
 Department of Computer Sciences  
 The University of Texas at Austin  
 Austin, TX 78712-1188  
 USA