WIRING SWITCHES TO LIGHT BULBS

STEPHEN M. BUCKLEY AND ANTHONY G. O'FARRELL

ABSTRACT. Given n buttons and n bulbs so that the ith button toggles the ith bulb and at most two other bulbs, we compute the sharp lower bound on the number of bulbs that can be lit regardless of the action of the buttons.

1. INTRODUCTION

The following problem was posed in the 2008 Irish Intervarsity Mathematics Competition:

> In a room there are 2008 bulbs and 2008 buttons, both sets numbered from 1 to 2008. For $1 \leq i \leq 2008$, pressing Button i changes the on/off status of Bulb i and one other bulb (the same other bulb each time). Assuming that all bulbs are initially off, prove that by pressing the appropriate combination of buttons we can simultaneously light at least 1340 of them. Prove also that in the previous statement, 1340 cannot be replaced by any larger number.

This problem, henceforth referred to as the *Prototype Problem*, can be generalized in a variety of ways:

(a) Most obviously, "2008" can be replaced by a general integer n.
(b) We can consider more general wirings W, where each button changes the on/off status of a (possibly non-constant) number of bulbs.
(c) We may consider initial configurations c where not all of the bulbs are off.
(d) We however insist that the numbers of buttons and bulbs are equal, and that Button i changes the on/off status of Bulb i, $1 \leq i \leq n$.

Such problems are rather closely related to the type of problem known as MAX-XOR-SAT in Computer Science. We discuss this connection in more detail in the next section.

Figure 1 is a sketch of a typical wiring.

Before we continue, let us introduce a little notation. For a fixed wiring W, where the initial configuration of the bulbs is given by c, let $M(W, c)$ be the maximum number of bulbs that can be lit by pressing any combination of the buttons.

Suppose $n, m \geq 1$. Let $\mu(n, m)$ be the minimum value of $M(W, c)$ over all wirings W of n buttons and bulbs, where Button i is connected to *at most* m bulbs, including Bulb i, for each $1 \leq i \leq n$, and initially all bulbs are off (which we write as "$c = 0$"). If additionally $n \geq m$, let $\mu^*(n, m)$ be the minimum value of $M(W, c)$ over all wirings

Date: January 26, 2011.
2000 *Mathematics Subject Classification.* Primary: 05D99. Secondary: 68R05, 94C10.
Key words and phrases. MAX-XOR-SAT, Hamming distance.
The first author was partly supported by Science Foundation Ireland. Both authors were partly supported by the European Science Foundation Networking Programme HCAA.

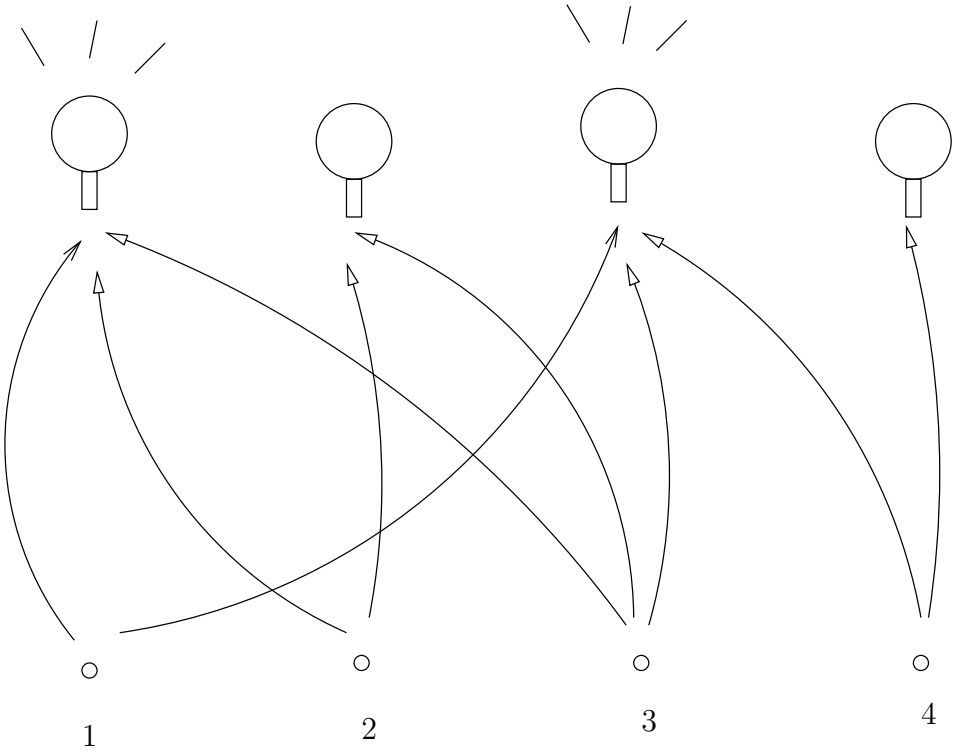

FIGURE 1. A Wiring

W of n buttons and bulbs, where Button i is connected to *exactly* m bulbs, including Bulb i, for each $1 \le i \le n$, and $c = 0$. Thus the Prototype Problem is to show that $\mu^*(2008, 2) = 1340$.

We define $\mu(n) = \mu(n, n)$, which trivially equals $\mu(n, m)$ for all $m > n$. Thus $\mu(n)$ is the minimum value of $M(W, 0)$, over all wirings of the n buttons, subject only to condition (d) above.

We also define $\nu(n, m)$, $\nu^*(n, m)$, and $\nu(n)$ in a similar manner to $\mu(n, m)$, $\mu^*(n, m)$, and $\mu(n)$, respectively, except that we take the minima over all possible initial configurations c, rather than taking $c = 0$. In this paper, we are mainly interested in $\mu(n, m)$ and $\mu^*(n, m)$, and we compute these functions for $m \le 3$. However the more easily calculated ν-variants will be useful, so we compute them in all cases.

Our first theorem gives formulae for $\mu(n, 2)$ and $\mu^*(n, 2)$; note that $\mu(n, 2) = \mu^*(n, 2)$ except when $n \equiv 1 \mod 3$.

Theorem 1.1. *Let $n \in \mathbb{N}$.*

(a) $\mu(n, 2) = \left\lceil \dfrac{2n}{3} \right\rceil$.

(b) *If $n \ge 2$, then $\mu^*(n, 2) = 2 \left\lceil \dfrac{n}{3} \right\rceil$ is the least even integer not less than $\mu(n, 2)$.*

Next we give formulae for $\mu(n, 3)$ and $\mu^*(n, 3)$.

Theorem 1.2. *Let $n \in \mathbb{N}$.*

(a) $\mu(n, 3) = \mu(n, 2)$.

(b) *If $n \geq 3$, then*

$$\mu^*(n,3) = \begin{cases} 4k-1, & n = 6k-3 \text{ for some } k \in \mathbb{N}, \\ \mu(n,3), & \text{otherwise.} \end{cases}$$

Note that $\mu^*(n,3) = \mu(n,3) + 1$ in the exceptional case $n = 6k-3$.

We discuss $\mu(n,m)$ and $\mu^*(n,m)$ in the case $n > 3$ in a separate paper [1]. Let us note here only that $\mu(n,m)$ and $\mu^*(n,m)$ are no longer asymptotic to $2n/3$ for large n, when $m \geq 4$. For instance, we prove in [1] that $\mu(n,4)$ is asymptotic to $4n/7$, and that $\liminf_{n\to\infty} \mu(n)/n = 1/2$.

After some preliminaries in the next section, where we also discuss the connection between this problem and MAX-XOR-SAT, we prove general formulae for $\nu(n,m)$ and $\nu^*(n,m)$ in Section 3. We then prove Theorem 1.1 in Section 4 and Theorem 1.2 in Section 5.

We wish to thank David Malone for pointing out the connection between our results and SAT.

2. Notation and terminology

The notation and terminology introduced in this section will be used throughout the paper. We begin by recasting our problem. First note that we can replace the twin notions of buttons and bulbs with the single notion of vertices: when a vertex is pressed, the on/off state of that vertex and some other vertices is switched. The vertex set $S := \{1, \ldots, n\}$ is associated with a directed graph G: we draw an edge from vertex i to each vertex $j \neq i$ whose on/off status is altered by pressing vertex i. Figure 2 shows a representation of the directed graph corresponding to the wiring in Figure 1. Notice

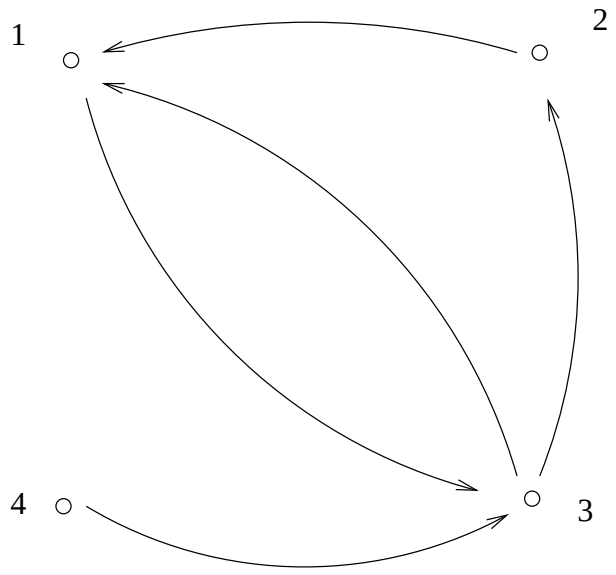

Figure 2. Graph for Figure 1

that we do not include a loop from each vertex to itself, even though it is understood that a given switch always switches the corresponding bulb.

Associated with a given directed graph G is the *edge function* $F : S \to 2^S$, where $j \in F(i)$ if $j = i$ or if there is an edge from i to j, and the *backward edge function* $F^{-1} : S \to 2^S$, where $j \in F^{-1}(i)$ if $j = i$ or if there is an edge from j to i. We extend the definitions of F and F^{-1} to 2^S in the usual way: $F(T)$ and $F^{-1}(T)$ are the unions of $F(i)$ or $F^{-1}(i)$, respectively, over all $i \in T \subset S$. We say that $T \subset S$ is *forward invariant* if $F(T) \subset T$, or *backward invariant* if $F^{-1}(T) \subset T$. We denote by G_T the subgraph of G consisting of the vertices in T and all edges between them.

If we examine the effect of a finite sequence of vertex presses $i_1, \dots, i_k$, on a fixed vertex i_0, it is clear that the final on/off state of vertex i_0 depends only on its initial state and the parity of the number of indices j, $1 \le j \le k$, for which $i_0 \in F(i_j)$. In particular, the order of the vertices in our finite sequence is irrelevant to the final state of i_0. Since this is true for each vertex, we readily deduce the following:

- The order of a finite sequence of vertex presses is irrelevant to the final on/off states of all vertices.
- We may as well assume that each vertex is pressed at most once, since pressing it twice produces the same effect as not pressing it at all.

Thus instead of talking about a *finite sequence* of vertex presses, we can talk about a *set* of vertex presses and represent this set as an n-dimensional column vector $x \in \mathbb{F}_2^n$ (where $\mathbb{F}_2 = \{0, 1\}$ denotes the field with two elements), with $x_i = 1$ if and only if vertex i is pressed once and $x_i = 0$ if it is not pressed at all. Similarly, we represent the initial on/off state of the vertices by a column vector $c \in \mathbb{F}_2^n$, with $c_i = 1$ if and only if vertex i is initially lit. Lastly, we represent the wiring W as an element in $M(n, n; \mathbb{F}_2)$, the space of $n \times n$ matrices over $\mathbb{F}_2$. Specifically, $W = (w_{i,j})$, where $w_{i,j} = 1$ if and only if vertex j affects the on/off status of vertex i; we insist that $w_{i,i} = 1$ for all $i \in S$. The *degree of vertex* i, $\deg(i)$, is the number of 1s in the ith column of W (or equivalently the cardinality of $F(i)$), and the *degree of* W, $\deg(W)$, equals $\max\{\deg(i) : i \in S\}$.

We use a t-superscript for matrix transposition, and I_n is the $n \times n$ identity matrix.

For $u \in \mathbb{F}_2^n$, we define $|u|$ to be the Hamming "norm" or Hamming distance from u to the origin, i.e. the number of 1 entries in u. With the above definitions for x, c, W, the vector $v = Wx + c \in \mathbb{F}_2^n$ is such that $v_i = 1$ if and only if vertex i is lit, assuming we have initial configuration c, wiring W, and vertex presses given by x. Moreover, $|Wx + c|$ is the number of lit vertices. The function $M(W, c)$ defined in the Introduction can now be described as $\max\{\, |Wx + c| : x \in \mathbb{F}_2^n \,\}$.

For $n, m \ge 1$, we define $A(n, m)$ to be the set of matrices in $W \in M(n, n; \mathbb{F}_2)$ that have 1s all along the diagonal and satisfy $\deg(W) \le m$. If also $n \ge m$, we define $A^*(n, m)$ to be the set of matrices in $A(n, m)$ for which $\deg(i) = m$, for all $i \in S$. These classes of matrices are the classes of admissible wirings for the functions defined in the Introduction:

$$\begin{aligned}
\mu(n, m) &= \min\{M(W, 0) \mid W \in A(n, m)\}, \\
\mu^*(n, m) &= \min\{M(W, 0) \mid W \in A^*(n, m)\}, \\
\nu(n, m) &= \min\{M(W, c) \mid W \in A(n, m),\ c \in \mathbb{F}_2^n\}, \\
\nu^*(n, m) &= \min\{M(W, c) \mid W \in A^*(n, m),\ c \in \mathbb{F}_2^n\},
\end{aligned}$$

The largest class of admissible wirings on n vertices that interests us is $A(n) := A(n, n)$. This gives rise to the numbers $\mu(n) := \mu(n, n)$ and $\nu(n) := \nu(n, n)$, as defined in the Introduction. It is convenient to define $\mu(0, m) = 0$ for all $m \in \mathbb{N}$.

Although the Hamming distance is a central part of the problems under consideration, these problems are on the surface quite different from those in coding theory, since we are looking for wirings that minimize the maximum distance from the origin of Mx, $x \in \mathbb{F}_2^n$, whereas in coding theory we are looking for codes that maximize the minimum distance between codewords. However, it is shown in [1] that Sylvester-Hadamard matrices, which are known to give rise to Hadamard codes that possess a certain optimality property, also give rise to certain optimal wirings.

We say that a subgraph H of G with k vertices is a *complete subgraph (on k vertices)* if there is an edge from every vertex of H to every other vertex of H. For brevity, we call a complete subgraph on k vertices a C_k from now on, and a C_k *set* is just the set of vertices of a C_k.

The problems under consideration in this paper are closely related to MAX-XOR-SAT problems in Computer Science. These problems are in the general area of propositional satisfiability (*SAT*). Specifically we want to assign values to Booloean variables so as to maximize the number of clauses that are true, where each clause is composed of a set of variables connected by XORs. Since XOR in Boolean logic corresponds to addition mod 2, this problem can be written in our notation as follows: given a matrix $W \in M(N, n; \mathbb{F}_2)$, we wish to choose a *variables vector* $x = (x_i : 1, \ldots, x_n) \in \mathbb{F}_2^n$ so as to maximize the Hamming norm $|Wx|$; the N entries in $Wx \in \mathbb{F}_2^N$ are the *clauses*. Thus the goal is to compute $M(W, 0)$.

XOR-SAT and MAX-XOR-SAT has been studied extensively in recent years; see for instance [2], [3], [4], [5]. Algorithms for solving such problems are useful in cryptanalysis [6], [7].

The relationship between MAX-XOR-SAT and our wiring problem is plain to see, so let us instead mention the differences:

- MAX-XOR-SAT is concerned with finding $M(W, 0)$ for a fixed but arbitrary W, rather than seeking the minimum of $M(W, 0)$ over a class of admissible Ws. The main problems in MAX-XOR-SAT revolve around the efficiency of the computation of $M(W, 0)$ for large n rather than the computation of a minimum for all n.
- In MAX-XOR-SAT, there is no requirement that $N = n$, and so no matching of clauses with variables (or bulbs with buttons in our terminology) and no requirement that $w_{ii} = 1$.
- In MAX-XOR-SAT and other SAT problems, the typical simplifying assumption is that there are either exactly, or at most, m variables in each clause. Thus in SAT we typically bound the Hamming norms of the rows of W, while in our wiring problem we bound the Hamming norms of the columns of W.

In spite of the differences, we would hope that the lower bounds in $M(W, 0)$ given by our results might be of some interest to MAX-XOR-SAT researchers.

3. Formulae for ν and ν^*

Given $n \geq m$, the following inequalities are immediate:

$$\nu(n, m) \leq \nu^*(n, m) \leq \mu^*(n, m) \tag{3.1}$$

$$\nu(n, m) \leq \mu(n, m) \leq \mu^*(n, m) \tag{3.2}$$

We now establish a lower bound for $M(W, c)$.

Lemma 3.3. *Let $n \in \mathbb{N}$. For all $W \in A(n)$ and $c \in \mathbb{F}_2^n$, the mean value of $|Mx+c|$ over all $x \in \mathbb{F}_2^n$ is $n/2$. In particular, $M(W, c) \geq n/2$ and $M(W, c) > n/2$ if the cardinality of $\{i \in [1, n] \cap \mathbb{N} \mid c_i = 1\}$ is not $n/2$.*

Proof. Fix W and c. Let $S_i = \{x \in \mathbb{F}_2^n \mid x_i = 0\}$ and $T_i = \mathbb{F}_2^n \setminus S_i$. Both S_i and T_i have cardinality 2^{n-1} and, since pressing vertex i toggles its own on/off status, the number of $x \in S_i$ with i lit (i.e. $(Wx + c)_i = 1$) equals the number of $x \in T_i$ with i unlit (i.e. $(Wx + c)_i = 0$). Thus letting x range over $\mathbb{F}_2^n$, the mean value of v_i is $1/2$, and the mean value of $|Wx + c|$ is $n/2$. The last statement in the lemma follows easily. □

The above lemma is a key tool in proving the following result which gives the general formula for $\nu(n, m)$ and $\nu^*(n, m)$. In this result, we ignore the case $m = 1$ since trivially $\nu(n, 1) = \nu^*(n, 1) = n$.

Theorem 3.4. *Let $n, m \in \mathbb{N}$, $m > 1$.*

(a) $\nu(n) = \nu(n, m) = \left\lceil \dfrac{n}{2} \right\rceil$.

(b) *If $n \geq m$, then*

$$\nu^*(n, m) = \begin{cases} \nu(n, m) + 1, & \text{if } n \text{ is even and } m \text{ odd,} \\ \nu(n, m), & \text{otherwise.} \end{cases}$$

In particular, $\nu^*(n, 2) = \nu^*(n) = \nu(n)$ for all $n > 1$.

Proof. We will prove each identity by showing that the right-hand side is both a lower and an upper bound for the left-hand side.

By Lemma 3.3, $M(W, c) \geq \left\lceil \dfrac{n}{2} \right\rceil$ for all $W \in A(n)$ and $c \in \mathbb{F}_2^n$. This global lower bound yields the desired lower bound for $\nu(n)$ and *a fortiori* for $\nu(n, m)$ and for $\nu^*(n, m)$ except in the case where n is even and m is odd.

Fix $c \in \mathbb{F}_2^n$ and $W \in A^*(n, m)$ for some odd $m > 1$ and $n \geq m$. Each vertex press must change the parity of the number of lit vertices and, since the mean value of $|Wx + c|$ is $n/2$, it follows that $|Wx + c| > n/2$ for some $x \in \mathbb{F}_2^n$. Since $\nu(n, m) = n/2$ if n is even, we deduce that $\nu^*(n, m) \geq \nu(n, m) + 1$ if n is even and m odd.

To prove the reverse inequalities, we take as our initial configuration the *even indicator vector* $e \in \mathbb{F}_2^n$ defined by $e_i = 1$ when i is even, and $e_i = 0$ when n is odd. We split the set of integers between 1 and n into pairs $\{2k - 1, 2k\}$, $1 \leq k \leq n/2$, with n being unpaired if n is odd; corresponding to the pairs of integers, we have *pairs of rows* in the wiring matrix W and *pairs of vertices*. For each proof of sharpness, we will define $W = (w_{i,j})$ such that $M(W, e)$ equals the desired lower bound. Pressing vertex j has no effect on the pair of vertices $2k - 1$ and $2k$ if $w_{2k-1,j} = w_{2k,j} = 0$, and it toggles both of them if $w_{2k-1,j} = w_{2k,j} = 1$. Since initially one vertex in each pair is lit, this remains true regardless of what vertices we press if the corresponding pair of rows are equal to each other (as will be the case for most pairs of rows). Thus, in calculating $M(W, e)$, we can ignore all pairs of equal rows, for which the corresponding vertex presses leaves the number of lit vertices unchanged, and we only have to consider the vertices that do not come in equal pairs.

For $t \in \{0, 1\}$, we denote by $t_{p\times q}$ the $p \times q$ matrix all of whose entries equal t, and let $t_p = t_{p\times p}$. The matrix 1_p should not be confused with the identity matrix I_p.

To finish the proof of (a), it suffices to show that $\nu(n,2) \leq \left\lceil \frac{n}{2} \right\rceil$. Define the $n \times n$ block diagonal matrix

$$W = \begin{cases} \mathrm{diag}(1_2, \ldots, 1_2), & n \text{ even}, \\ \mathrm{diag}(1_2, \ldots, 1_2, 1_1), & n \text{ odd}, \end{cases} \tag{3.5}$$

In case $n = 9$, this matrix corresponds to the wiring of nine switches and bulbs represented by Figure 3. In this figure, the boxes labelled by the number 2 represent complete directed graphs on two vertices, and the small circle represents a single vertex. We shall always indicate a C_v subgraph by a box labelled v.

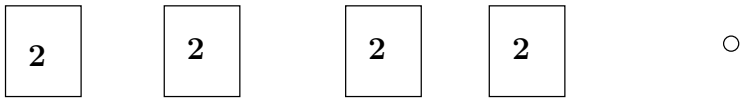

FIGURE 3. $n = 9$

Then $W \in A(n,2)$ and $M(W,e) = \left\lceil \frac{n}{2} \right\rceil$. To see this, note that rows $2k-1$ and $2k$ of W are equal to each other for each $1 \leq k \leq n/2$. Thus when n is even, $|Wx + e|$ is independent of x, while it toggles between the two values r and $r-1$ when $n = 2r-1$ is odd, due to the change in the state of vertex n each time that vertex is pressed.

It remains to prove that the desired formula for $\nu^*(n,m)$ is also an upper bound for $\nu^*(n,m)$ when $n \geq m > 1$. Suppose first that $n - m$ is even. First define the block diagonal matrix $W' \in A(n,m)$ by the formula $W' = \mathrm{diag}(1_2, \ldots, 1_2, 1_m)$, where there are $(n-m)/2$ copies of 1_2. We modify $W' = (w'_{i,j})$ to get a matrix $W = (w_{i,j}) \in A^*(n,m)$ by adding $m-2$ 1s to the end of the first $n-m$ columns, i.e. let

$$w_{i,j} = \begin{cases} 1, & i > n-m+2 \text{ and } j \leq n-m, \\ w'_{i,j}, & \text{otherwise} \end{cases}$$

In case $n = 9$ and $m = 3$, the matrix W corresponds to a wiring of the kind indicated in Figure 4. In this diagram, the boxes indicate complete subgraphs having two or three vertices, as indicated. A single arrow coming from a C_2 box indicates an edge from *each* of the two vertices in the box and going to *the same* vertex in the C_3. The target vertex may be the same or different for the three C_2's, but the vertices in a given C_2 share the same target. In general, in our diagrams, we will use the convention that all the switches corresponding to vertices in a given C_v box produce exactly the same effect. Notice that nonisomorphic graphs may correspond to the same "box diagram", in view of the fact that a box diagram is not specific about the targets of some arrows.

All paired rows of W are equal, so if n and m are both even, then $|Wx + e| = n/2$ for all $x \in \mathbb{F}_2^n$, whereas if n and m are both odd, the value of $|Wx + e|$ is either $(n+1)/2$ or $(n-1)/2$, depending on the parity of $|x_i|$. In either case, we have found a matrix $W \in A^*(n,m)$ with $M(W,e) = \nu(n,m)$, and so $\nu^*(n,m) = \nu(n,m)$.

Suppose next that n is odd and m even, with $n > m+1$. We first define the block diagonal matrix $W' \in A(n,m)$ by the formula $W' = \mathrm{diag}(1_m, 1_2, \ldots, 1_2, W_3)$, where there

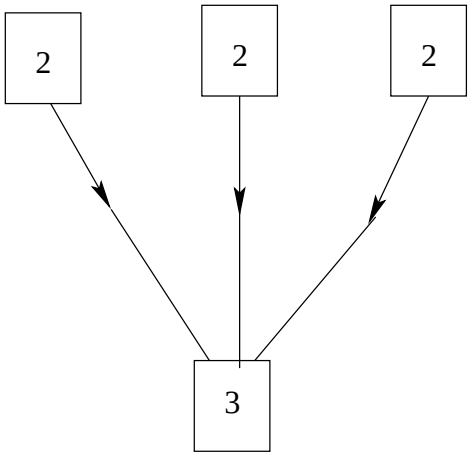

FIGURE 4. $n = 9$, $m = 3$

are $(n - m - 3)/2$ copies of 1_2 and

$$W_3 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} . \tag{3.6}$$

and then define $W = (w_{i,j})$ by the equation

$$w_{i,j} = \begin{cases} 1, & 3 \le i \le m \text{ and } j > m, \\ w'_{i,j}. & \text{otherwise} \end{cases} \tag{3.7}$$

The corresponding wiring is indicated schematically in Figure 5.

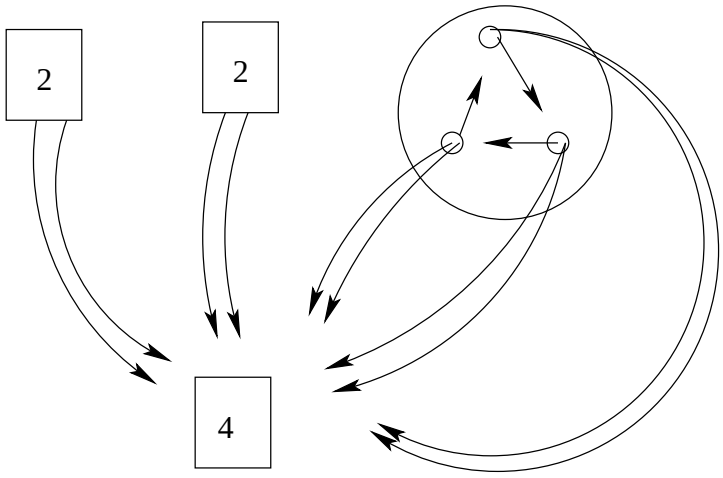

FIGURE 5. $n = 11$, $m = 4$

The circled subgraph corresponds to the matrix W_3.

The first $n - 3$ rows can be split into duplicate pairs as before, so the associated pairs of vertices will always be of opposite on/off status and the number of them that is lit is always $(n - 3)/2$.

Initially two of the last three vertices are lit. Since m is even, the parity of the number of lit vertices is preserved, and so no more than two of the last three vertices can be lit. Thus $M(W, e) = (n + 1)/2$ in this case, as required.

The case where m is odd and $n > m+1$ is even, is similar. We first define $W' \in A(n, m)$ by the formula $W' = \mathrm{diag}(1_m, W_3, 1_2, \ldots, 1_2)$, and then define $W = (w_{i,j})$ from W' by (3.7). The corresponding wiring is indicated schematically in Figure 6.

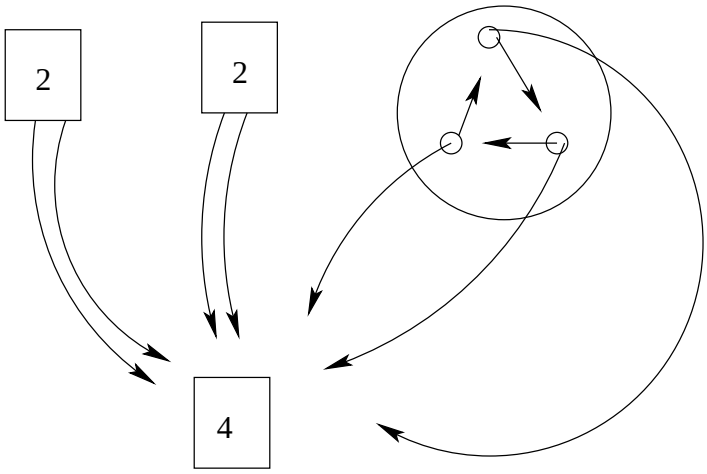

FIGURE 6. $n = 10$, $m = 3$

There are four unpaired rows, namely rows i, $m \le i \le m + 3$. By an analysis similar to the previous case, at most three of these vertices can be lit (namely vertex m and at most two of the other three vertices), and half of the remaining $n-4$ vertices are always lit. It follows that $M(W, e) = (n + 2)/2$, as required.

Finally if $n = m + 1$, we define W to be the block diagonal matrix

$$W = \begin{pmatrix} 1_{(m-1)\times m} & 1_{(m-1)\times 1} \\ 1_{1\times m} & 0_{1\times 1} \\ 0_{1\times m} & 1_{1\times 1} \end{pmatrix}$$

See Figure 7.

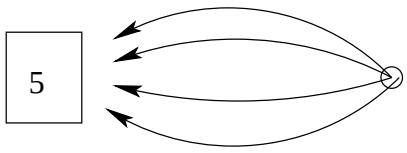

FIGURE 7. $n = 6$, $m = 5$

The first m or $m - 1$ rows are paired, depending on whether m is even or odd, respectively. Thus $M(W, e) \le 1 + m/2$ if m is even, or $M(W, e) \le 2 + (m - 1)/2$ if m is odd, as required. □

Generalizing an idea used in the above proof, we see that if W and c have block forms

$$W = \begin{pmatrix} W_a & 0 \\ 0 & W_b \end{pmatrix} \qquad c = \begin{pmatrix} c_a \\ c_b \end{pmatrix},$$

then

$$M(W, c) = M(W_a, c_a) + M(W_b, c_b)\,. \tag{3.8}$$

This readily yields the following:

Corollary 3.9. *If λ is any one of the four functions μ, μ^*, ν, or ν^*, then it is sublinear in the first variable:*

$$\lambda(n_1 + n_2, m) \le \lambda(n_1, m) + \lambda(n_2, m)\,, \tag{3.10}$$

as long as this equation makes sense (i.e. we need $n_1, n_2 \ge m$ if $\lambda = \mu^*$ or $\lambda = \nu^*$).

4. The case $m = 2$

Proof of Theorem 1.1. Trivially $\mu(1, 2) = 1$, and it is easy to check that $\mu(2, 2) = 2$. Taking W_3 as in (3.6), we see that $M(W_3, 0) = 2$, and so $\mu(3, 2) \le \mu^*(3, 2) \le 2$. By combining (3.10) with these facts, we see that for $k \in \mathbb{Z}$, $k \ge 0$, and $i \in \{0, 1, 2\}$,

$$\mu(3k + i) \le k\mu(3, 2) + \mu(i, 2) \le 2k + i\,.$$

Since $2k + i = \left\lceil \dfrac{2(3k + i)}{3} \right\rceil$, this gives the sharp upper bound for $\mu(n, 2)$. The corresponding sharp upper bound for $\mu^*(n, 2)$ follows similarly when $n \ge 1$ has the form $3k$ or $3k + 2$, $k \ge 0$. If $n = 3k + 1$, $k \ge 1$, only a small change is required to the μ-proof to get a proof of the sharp μ^* upper bound:

$$\mu^*(3k + 1, 2) \le (k - 1)\mu^*(3, 2) + 2\mu^*(2, 2) = 2k + 2\,.$$

It remains to show that we can reverse the above inequalities. We first examine the reverse inequalities for μ^*, so fix $W \in A^*(n, 2)$. Writing $F : S \to 2^S$ for the edge function, where $S := \{1, \dots, n\}$, we get a well-defined function $f : S \to S$ by writing $f(i) = j$ whenever there is an edge from i to j in the associated graph G. For a dynamical system on any finite set, every point is either periodic or preperiodic. In our context, this just means that if we apply f repeatedly to any initial vertex $i \in S$, then we eventually get a repeat of an earlier value, and from then on the iterated values of f go in a cycle.

Note that the topological components of G do not "interfere" with each other: the vertices in any one component affect only the on/off status of vertices in this component, so maximizing the number of lit vertices can be done one component at a time (alternatively, this follows from (3.8) after reordering of the vertices).

A component of the graph G consists of a central circuit containing two or more vertices, with perhaps some directed trees, each of which leads to some vertex of the circuit, which we call the *root* of that tree. Starting from the outermost vertices of such a tree (those that are not in the range of f) and working our way down to the root, it is not hard to see that we can simultaneously light all vertices in each of these trees. Having done this, some of the vertices in the central circuit may not be lit up. We follow the vertices around the circuit in cyclic order, pressing each vertex that is unlit when we reach it until we have gone fully around the circuit. It is clear that at this stage at most one vertex in the circuit is unlit, and all the associated trees are still fully lit.

Note that any single vertex press either leaves the number of lit vertices in a given component unchanged, or changes that number by 2. Since initially all vertices are unlit,

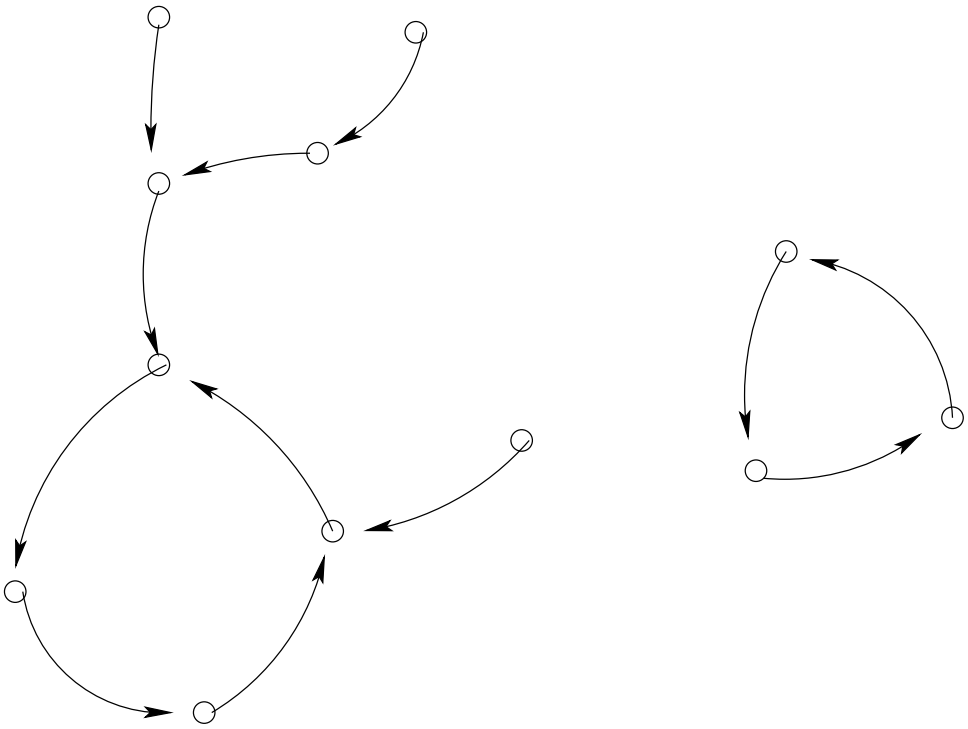

FIGURE 8. 'Dynamics' of $m = 2$

it follows that the number of lit vertices in a component is always even. It therefore follows that in a component of even cardinality all vertices can be lit, while in a component of odd cardinality all except one can be lit.

Thus it follows that to minimize $M(W, 0)$ we need to maximize the number of components of odd cardinality (necessarily at least 3), and that the maximum proportion of lit vertices in any one component is at least $2/3$ (with equality only for components of cardinality 3). Thus $\mu^*(n, 2) \geq \lceil 2n/3 \rceil$, which gives the required lower bound except when $n = 3k + 1$, $k \in \mathbb{N}$. Since G has $n = 3k + 1$ vertices and all components have at least two vertices, it can have at most $k - 1$ components of odd cardinality, yielding the desired estimate $\mu^*(3k + 1, 2) \geq 3k + 1 - (k - 1) = 2k + 2$. Thus $\mu^*(n, 2)$ is given by the stated formula in all cases.

For μ, the above proof goes through with little change, except that components can now be singletons. Singleton components can always be lit, so $\mu(n, 2) \geq \lceil 2n/3 \rceil$, as required. □

Note that although singleton components do not contribute unlit vertices, they do allow us to get k, rather than just $k - 1$, components of odd cardinality at least 3 when $n = 3k + 1$. This accounts for the difference between $\mu(n, 2)$ and $\mu^*(n, 2)$ in this case.

5. Pivoting and the case $m = 3$

In preparation for the proof of Theorem 1.2, we introduce the concept of *pivoting*. Pivoting about a vertex i, $1 \leq i \leq n$, is a way of changing the given wiring W to a special wiring W^i such that $M(W^i, c) \leq M(W, c)$. Additionally, pivoting preserves the classes $A(n, m)$ and $A^*(n, m)$.

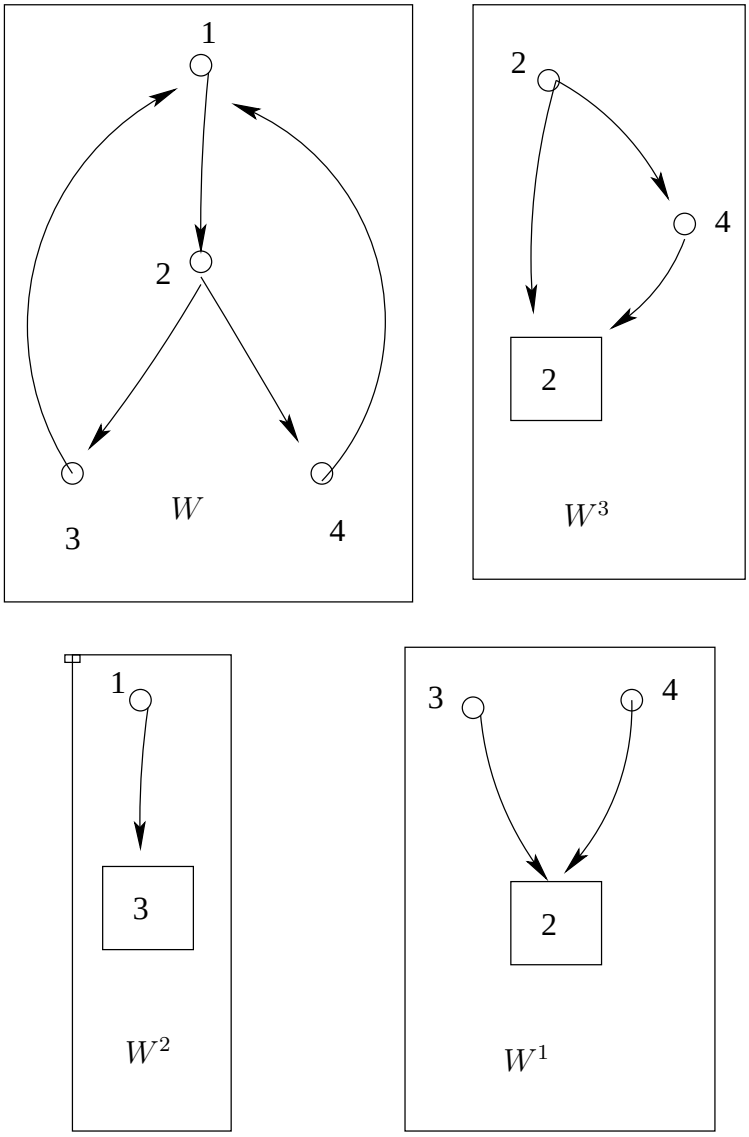

FIGURE 9. Pivoting

Fixing a wiring $W = (w_{i,j})$ and initial configuration c, and let $F : S \to 2^S$ denotes the edge function associated to W, where $S = \{1, \dots, n\}$. Given $i \in S$, let $M_i = M(W^i, c)$ where the *pivoted wiring matrix* W^i is defined by the condition that its jth column equals the ith column of W if $j \in F(i)$, and equals the jth column of W otherwise. In other words, W^i rewires the system so that pressing the jth vertex has the same effect as pressing the ith vertex in the original system whenever $j \in F(i)$. On the other hand, it is easy to see that M_i is the maximum value of $|Wx + c|$ over all vectors x such that $x_j = 0$ whenever $j \in F(i) \setminus \{i\}$. In particular, $M_i \le M(W, c)$.

Pivoting about i, as defined above, is a process with several nice properties:

- it does not increase the value of M: $M(W^i, c) \le M(W, c)$;
- it preserves membership of the classes $A(n, m)$ and $A^*(n, m)$;
- if F^i is the edge function of W^i, then $F^i(i) = F(i)$ is a forward invariant complete subgraph of the associated graph G^i.

It is sometimes useful to pivot *partially* about i: given $T \subset S$, and $i \in S$, we define W' by replacing the jth column of W by its ith column whenever $j \in F(i) \setminus T$. Such *pivoting about i with respect to T* satisfies the same non-increasing property, preserves membership in $A(n,m)$ and $A^*(n,m)$, and $F(i)\setminus T$ is a (not necessarily forward invariant) complete subgraph of the associated graph G'.

Pivoting is the key trick in the proof of the following lemma.

Lemma 5.1. *Let $m \geq 2$ and $n \geq 1$. Then either $\mu(n+m,m) = \mu(n+m,m-1)$, or*

$$\mu(n+m,m) \geq \mu(n,m) + \nu(m,m) = \mu(n,m) + \left\lceil \frac{m}{2} \right\rceil .$$

Proof. Suppose $\mu(n+m,m) < \mu(n+m,m-1)$, and let $W \in A(n+m,m)$ be such that $M(W,0) = \mu(n+m,m)$. Then W has a vertex i of degree m. By minimality of W, pivoting about i gives $W^i \in A(n,m)$ with $M(W^i,0) = \mu(n+m,m)$ (cf. Figure 10. The loop marked $n-m$ just indicates an unspecified subgraph of order $n-m$.). For the wiring W^i, we first press a set of vertices in

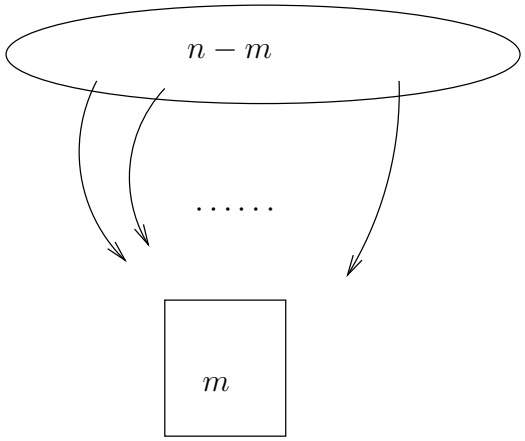

FIGURE 10. W^i

$S \setminus F(i)$ so as to maximize the number of lit vertices in $S \setminus F(i)$, and then we press vertex i if fewer than half of the vertices in $F(i)$ are lit. By forward invariance of $F(i)$, the result follows. □

Proof of Theorem 1.2(a). Trivially, we have that $\mu(n,3) \leq \mu(n,2)$, with equality if $n < 3$. It is also immediate that $\mu(3,3) = \mu(3,2) = 2$: any wiring that includes a vertex of degree 3 allows us to light all vertices by pressing the degree 3 vertex.

Suppose therefore that $\mu(n',3) = \mu(n',2)$ for all $n' < n$, where $n > 3$. Either this equation still holds when n' is replaced by n, or

$$\mu(n,2) = \mu(n-3,2) + 2 = \mu(n-3,3) + 2 = \mu(n-3,3) + \nu(3,3) \leq \mu(n,3) \leq \mu(n,2).$$

Here, the first equality follows from Theorem 1.1, the second from the inductive hypothesis, and the first inequality from Lemma 5.1. Since $\mu(n,2)$ is at both ends of this line, we must have $\mu(n,3) = \mu(n,2)$, and the inductive step is complete. □

For the proof of Theorem 1.2(b), we need another lemma.

Lemma 5.2. *Let $n, m, n' \in \mathbb{N}$, with $n \geq m$. Then*

$$\mu^*(n + n', m + 1) \leq \mu^*(n, m) + n' .$$

Proof. It suffices to prove the lemma subject to the restriction $n' \leq n$, since this case, the trivial estimate $\mu^*(n, m) \leq n$, and sublinearity (3.10) together imply the general case. Let us therefore assume that $n' \leq n$.

Let $V = (v_{i,j}) \in A^*(n, m)$ be such that $M(V, 0) = \mu^*(n, m)$. We now define a matrix $W = (w_{i,j}) \in A^*(n+n', m+1)$. First the upper left block of W is a copy of V, i.e. we let $w_{i,j} = v_{i,j}$ for all $1 \leq i, j \leq n$. Next, the $n' \times n$ block of W below V consists of copies of the $n' \times n'$ identity matrix; the last of these copies will be missing some columns unless n is a multiple of n'. Lastly, we define $w_{i,n+j} = w_{i,j}$ for all $1 \leq j \leq n'$. It is straightforward to verify that $W \in A^*(n + m', m + 1)$; note that the assumption $n' \leq n$ ensures that W has 1s along the diagonal. Refer to Figure 11 for a schematic. Note that vertex $6 + i$ has the same targets as vertex i, but these edges going to vertices other than 7 to 9 are not shown.

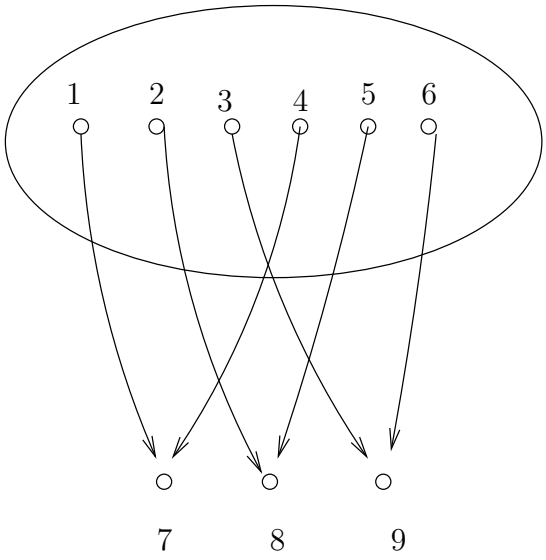

FIGURE 11. $n = 6$, $n' = 3$

Since all columns after the nth column are repeats of earlier columns, it suffices to consider what happens when we press only combinations of the first n vertices. Such combinations light at most $\mu^*(n, m)$ of the first n vertices, so we are done. □

Proof of Theorem 1.2(b). Lemma 5.2 ensures that if $k, i \in \mathbb{N}$, then $\mu^*(3k + i, 3) \leq \mu^*(3k, 2) + i = 2k + i$. This is the required sharp upper bound if $i = 1, 2$, since $2k+1 = \mu(3k+i, 2)$ in this case. On the other hand, $\mu^*(3k+i, 3) \geq \mu(3k+i, 3) = 2k+i$, for all $k, i \in \mathbb{N}$, and this gives the required converse for $i = 1, 2$.

It remains to handle the case where n is a multiple of 3. First we show that the lower bound $\mu^*(3k,3) \geq \mu(3k,3) = 2k$ is sharp when $k = 2k'$ is even. Letting

$$W_6 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix} \in A^*(6,3)\,, \tag{5.3}$$

we claim that $M(W_6, 0) = 4$. Assuming this claim, (3.10) gives the desired sharpness: $\mu^*(6k', 3) \leq k'\mu^*(6, 3) \leq k'M(W_6, 0) = 4k'$.

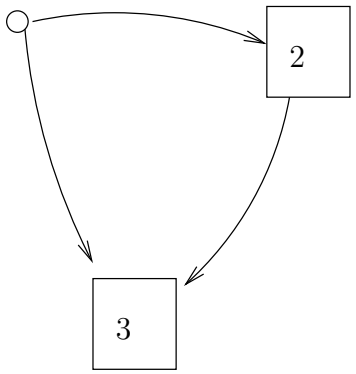

FIGURE 12. W_6

To establish the claim, it suffices to consider sets of vertex presses involving only vertices 1, 2, and 4. With this restriction, we proceed to list all eight possible values of x, and deduce that $M(W_6, 0) = 4$:

x^t	$(W_6x)^t$	$\lvert W_6x\rvert$
(0,0,0,0,0,0)	(0,0,0,0,0,0)	0
(1,0,0,0,0,0)	(1,1,0,0,1,0)	3
(0,1,0,0,0,0)	(0,1,1,1,0,0)	3
(1,1,0,0,0,0)	(1,0,1,1,1,0)	4
(0,0,0,1,0,0)	(0,0,0,1,1,1)	3
(1,0,0,1,0,0)	(1,1,0,1,0,1)	4
(0,1,0,1,0,0)	(0,1,1,0,1,1)	4
(1,1,0,1,0,0)	(1,0,1,0,0,1)	3

It remains to handle the case where $n = 6k' - 3$ for some $k' \in \mathbb{N}$. It is trivial that $\mu^*(3,3) = 3$. Next note that Lemma 5.2 ensures that for $k \geq 2$, $\mu^*(3k,3) \leq \mu^*(3k-3,2) + 3 = 2k + 1$, so we need to show that this is sharp if $k > 1$ is odd.

Supposing $\mu^*(n,3) = 2k$ for some fixed $n = 3k$, $k \in \mathbb{N}$, $k > 1$, we will prove that k must be even. Let $W = (w_{i,j}) \in A^*(n,3)$ be such that $M(W,0) = 2k$, let $S = \{1,\ldots,n\}$, and let $F : S \to 2^S$ be the edge function associated to W.

We can assume that W is additionally chosen so that the associated graph G has a maximal number of (disjoint) C_3's among all matrices $W' \in A^*(n,3)$ for which $M(W',0) =$

$2n/3$. The maximum number of C_3's is always positive since we can get a C_3 by pivoting about any one vertex; C_3 sets are pairwise disjoint and forward invariant, since each vertex in a C_3 uses up its two allowed outbound edges within the same C_3.

We define A to be the union of all the C_3 sets. If $i \in S \setminus A$, then $F(i) \cap A$ must be nonempty, since otherwise pivoting about i would create an extra C_3. Thus each $i \in S \setminus A$ has at most one edge from it to another vertex in $S \setminus A$. Suppose there is such a vertex i with $F(i)$ not a subset of A. Then we can pivot about i relative to A to get a C_2, and the only edges coming from this C_2 are single edges from both of its vertices to the same element in A. We repeat such pivoting of vertices relative to A to create more such C_2s until this is no longer possible. From now on W will denote this modified wiring matrix. We denote by B the union of the C_2 vertices and write $C = S \setminus (A \cup B)$, and we refer to each vertex in C as a C_1 (which it is, trivially).

We already know that there is an edge from each vertex in C to some vertex in A. If there is only a single edge from some $i \in C$ to $A \cup B$, then there must be an edge from i to some $j \in C$. Pivoting about i relative to $A \cup B$ (or equivalently, relative to A), we create a new C_2, contradicting the fact that this cannot be done. Thus there are two edges from each $i \in C$ to $A \cup B$. See Figure 13.

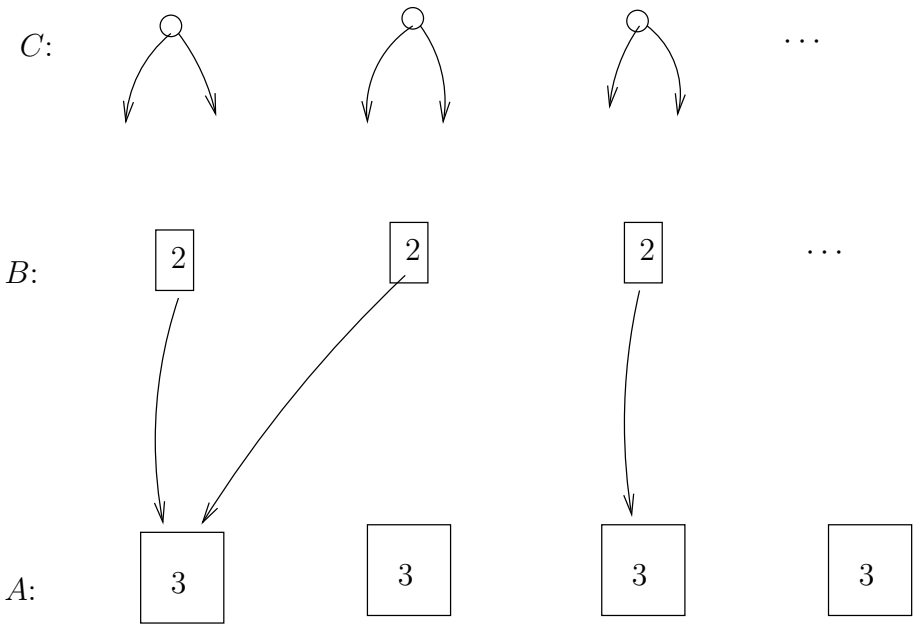

FIGURE 13.

We have shown that there are edges from C to $A \cup B$, and from B to A, but that both A and $A \cup B$ are forward invariant. Also, there are no links between elements in C, or between elements in distinct C_2's or in distinct C_3's. There are $3s$ elements in A, $2t$ elements in B, and u in C, for some integers s, t, u, and we have $3s + 2t + u = n$.

The forward invariance of both A and $A \cup B$ suggests two algorithms for lighting many of the vertices. The first is to begin by pressing all these vertices in C to light all these vertices. After this first step, we can ensure that at least one vertex in each C_2 is lit by pressing a vertex in any C_2 without a lit vertex. Finally, we ensure that at least two vertices are lit in each C_3 by pressing a vertex in any C_3 in which less

than two vertices are lit. Having done this, we have at least $2s + t + u$ lit vertices, so $2s + t + u \leq \mu^*(n, 3)$. Thus $6s + 3t + 3u \leq 3\mu^*(n, 3) = 2n$. When we compare this with the equation $6s + 4t + 2u = 2n$, we deduce that $t \geq u$.

An alternative algorithm for lighting the vertices is to first press one vertex in each C_2, thus lighting all C_2 vertices. As a second step, press a vertex in any C_3 in which less than 2 vertices are lit. Having done this, at least two vertices in each C_3 are lit as well as both vertices in each C_2. Consequently, $2s + 2t \leq \mu^*(n, 3) = 2n/3$. Thus $6s + 6t \leq 2n$, while $6s + 4t + 2u = 2n$. It follows that $u \geq t$, and so $u = t$.

Note that the first lighting algorithm gives at least $2s + 2t = 2n/3$ lit vertices, and it actually gives more than this number unless after the first step exactly one vertex in each C_2 is lit. Since any larger number contradicts $\mu^*(n, 3) = 2n/3$, there must be an edge from C to each C_2. But since the numbers of C_1's and of C_2's are equal, and there is at most one edge from each C_1 to B (since at least one edge from each C_1 goes to A), it follows that from each C_1 there is an edge to a C_2, and no other vertex in C is linked to the same C_2, i.e. we can pair off each C_1 with the unique C_2 to which it is linked in the graph. See Figure 14. We refer to the subgraph of G given by the union of a C_1 and

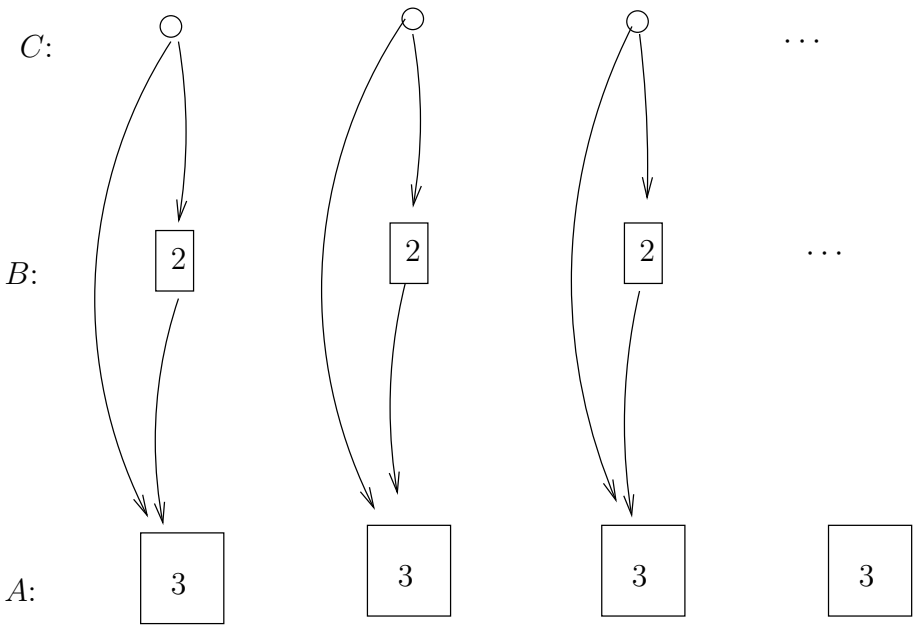

FIGURE 14.

a C_2 plus the edge between them as a $C_{1,2}$; the set of its three vertices is a $C_{1,2}$ set.

The second lighting algorithm will give more than $2s + 2t = 2n/3$ lit vertices unless the first step ends with one or two lit vertices in each C_3. Thus there is an edge from at least one C_2 to each C_3. Since any one C_2 is linked to only a single C_3, it follows that $t \geq s$.

We now define the *active vertices* to be the elements of a collection of vertices consisting of all C_1 vertices, together with one vertex from each C_2, and the *active edges* are all the edges coming from active vertices. When considering the effect of pressing sets of vertices in $B \cup C$, we can restrict ourselves to considering only sets of active vertices, hence the terminology.

To light more than two thirds of the vertices, it suffices to first light two vertices in every $C_{1,2}$ set in such a way that there is at least one C_3 that is either fully lit or fully unlit, since we can subsequently light two thirds of all vertices in all other C_3 sets, together with all vertices in the fully unlit or fully lit C_3, by pressing only C_3 vertices. Since each C_3 is forward invariant, we are done.

But given a $C_{1,2}$ set with all vertices unlit, pressing one or both of its active vertices leaves exactly two of its vertices lit. This gives us three ways of lighting two thirds of the vertices in that $C_{1,2}$ set, and this flexibility will be crucial to proving that n must be a multiple of 6. In particular, it means that for any given C_3, there must be an associated $C_{1,2}$ both of whose active vertices have edges leading to that C_3, since if this were not so, we could light two vertices in each $C_{1,2}$ without ever pressing a vertex linked to that C_3. Furthermore, even if a $C_{1,2}$ is doubly linked to a C_3, but the two active edges between them connect to the same vertex, then by pressing both active vertices, the on/off status of all vertices in the C_3 remains unchanged. Let us therefore say that a $C_{1,2}$ set with two active links to distinct vertices in a C_3 is *well linked* to that C_3 set. We say that they are *badly linked* if they are linked but not well linked.

It follows that S can be decomposed into a collection of $C_{1,2}$ sets, each of which is paired off with a distinct C_3 set to which it is well linked, plus $t - s$ extra $C_{1,2}$ sets that have not been paired off with any C_3, but are linked (well or badly) to some of the C_3's. We claim that if $t > s$ then the residual $C_{1,2}$ sets always allow us to arrange that at least one C_3 is fully lit or fully unlit after we light two vertices in every $C_{1,2}$. It follows the claim that n cannot be an odd multiple of 3, since then we would have $t - s > 0$, and we could light more than two thirds of the vertices.

Suppose therefore that $t > s$, and so there exists some particular C_3 with vertex set $D = \{a, b, c\}$, say, that has more than one $C_{1,2}$ linked to it, at least one of which is well linked. We wish to show that we can press one or both of the active vertices in each of the $C_{1,2}$'s linked to D while keeping D *in sync* (meaning that all three of its vertices are in the same on/off state).

Now D is initially in sync, and we can handle any two well-linked $C_{1,2}$'s while keeping D in sync. To see this, note that if the two pairs of active links go to the same pair of vertices in D, then we press all four active vertices in both $C_{1,2}$'s. If on the other hand, they do not go to the same pair of vertices then without loss of generality, one $C_{1,2}$ is linked to a and b and the other to b and c. By pressing three of the four active vertices, we can toggle the on/off status of all three vertices in D.

Since we can handle well-linked $C_{1,2}$'s two at a time, and we can handle badly linked ones one at a time, while keeping D in sync, we can reduce to the situation of having to handle only two or three $C_{1,2}$'s, with at least one of them well linked. We have already handled the case of two well-linked $C_{1,2}$'s, so assume that there are two $C_{1,2}$'s and exactly one is well linked, to a and b, say, while the other is badly linked, with either one or two links to a single vertex $v \in D$. By symmetry, we reduce to either of two subcases: if $v = a$, then we press one active vertex in both $C_{1,2}$'s that is connected to a, while if $v = c$, then we press three vertices so as to toggle the on/off status of all of D.

There remains the case of three linked $C_{1,2}$'s. If two are well linked and one badly linked, then we just handle the two well-linked ones together as above, and separately handle the badly linked one. Finally, all three may be well linked. If all three $C_{1,2}$'s link to the same pair of vertices, a and b, say, then we press both active vertices in one of them and one in the other two, to ensure that both a and b are toggled twice (and so

unchanged). If two $C_{1,2}$'s link to the same pair of vertices, a and b, say, and the third links to b and c, say, then we can press one vertex in each $C_{1,2}$ to ensure that all three vertices in D are toggled once. Finally if no two $C_{1,2}$'s leads to the same pair of vertices, then one leads to a, b, another to b, c, and a third to c, a. We can press all six of the active vertices so as to toggle each of a, b, c twice. This finishes the proof of the theorem. □

Note that even when n is a multiple of 6, the above argument gives us some extra information: after suitable pivoting, any wiring $W \in A^*(n, 3)$ with $M(W, 0) = 2n/3$ must reduce to a collection of $C_{1,2}$'s each of which is well linked to a distinct C_3. Each associated subgraph with six vertices is a component of the full graph and is unique (up to relabeling of the vertices). Moreover it is the graph of the wiring W_6 in (5.3) so, after suitable pivoting, any wiring $W \in A^*(n, 3)$ with $M(W, 0) = 2n/3$ reduces to $n/6$ copies of W_6.

References

[1] S.M. Buckley and A.G. O'Farrell, Wiring switches to more light bulbs, in preparation.

[2] N. Creignou and H. Daudé, 'Satisfiability threshold for random XOR-CNF formulae', *Discrete Appl. Math.* **96-97** (1999), 41–53.

[3] N. Creignou and H. Daudé, 'Smooth and sharp thresholds for random k-XOR-CNF satisfiability', *Theoret. Informatics Appl.* **37** (2003), 127–147.

[4] N. Creignou, H. Daudé, and U. Egly, 'Phase Transition for Random Quantified XOR-Formulas', *Journal of Artificial Intelligence Research* **29** (2007), 1–18.

[5] H. Daudé and V. Ravelomanana, 'Random 2-XORSAT at the Satisfiability Threshold'. In *Proceedings of the 8th Latin American conference on Theoretical informatics*, 12–23, 2008.

[6] M. Dietzfelbinger, A. Goerdt, M. Mitzenmacher, A. Montanari, R. Pagh, and M. Rink, 'Tight Thresholds for Cuckoo Hashing via XORSAT', arXiv:0912.0287v2.

[7] M. Soos, K. Nohl, and C. Castelluccia, 'Extending SAT solvers to cryptographic problems'. In *SAT (2009)*, O. Kullmann, Ed., Lecture Notes in Computer Science 5584, Springer, 244–257.

Department of Mathematics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland

E-mail address: stephen.m.buckley@gmail.com, anthonyg.ofarrell@gmail.com