Button Madness

(aeb, following notes by Aart Blokhuis)

1 The game

Let Γ be a graph with a light bulb and a button at each vertex. Suppose that pushing the button at vertex x switches the state (on/off) of x and each of its neighbours. For which starting positions is it possible to switch all lights off? For which graphs is it possible to switch all lights off for each starting position?

Let Γ have adjacency matrix A. Our questions are equivalent to: Which vectors are in the row span of $I + A$ over $\mathbb{F}_2$? Does $I + A$ have full 2-rank?

Concerning the former, the all-1 vector $\mathbf{1}$ is always in the row span.

Lemma 1.1 *The diagonal of a symmetric binary matrix lies in its row span.*

Proof. Let d be the diagonal of the matrix M defined over $\mathbb{F}_2$. If $Mu = 0$, then $u^\top Mu = 0$ and hence $d^\top u = 0$ (since all non-diagonal contributions cancel by symmetry). Thus, if u is orthogonal to the row space of M, it is also orthogonal to its diagonal. □

Concerning the latter, we have

Lemma 1.2 *The matrix $I+A$ has full 2-rank if and only if Γ has an odd number of matchings.*

Proof. The matrix $I + A$ has full 2-rank precisely when its determinant is nonzero (mod 2). All terms in the expansion of the determinant cancel by symmetry except for those that are their own mirror image. And these correspond precisely to the matchings of Γ. □

We may group matchings in orbits under some group of automorphisms of Γ, and only count the number of orbits of odd size. For example, if Γ is the m-cube (of valency m, on 2^m vertices), then consider the translation group of order 2^m. All orbits have even size except for the the orbits of size 1, which are the empty matching and m complete matchings. It follows that $I + A$ has full 2-rank precisely when m is even.

2 Button Madness

Let $\Gamma = C_n \times C_n$, the $n \times n$ torus on n^2 vertices. The valency is 4, each button press switches 5 lights. The number n is called *mad* when $I + A$ does not have full 2-rank, or, equivalently, when there exist nonempty sets of buttons such that pushing all of them does leaves the state unchanged.

For $n = 4$ this is the 4-cube, so 4 is not mad.

Lemma 2.1 *If m is mad, and $m|n$, then n is mad.*

Proof. Repeat a pattern in the kernel of $I + A_m$ periodically to find a pattern in the kernel of $I + A_n$. □

Lemma 2.2 *If m is not mad, then neither is $2m$.*

Proof. If we push a button and its four neighbours, the effect is a 'double' cross. This means that we can play the $2m$-game as four disjoint copies of the m-game. □

Let us call a number *MAD* when it is mad, but not a proper multiple of a mad number. MAD numbers are 3, 5, 17, 31, 127, 257, 511, 683, 2047, 2731, ... The number 1 is not mad, but 3 is, because pressing all buttons on two rows (or all buttons on a row and then all on a column) leaves the position invariant.

3 Algebraic formulation

Let the vertex (i, j) correspond to the monomial X^iY^j. A position corresponds to a polynomial $f(X, Y)$ in the ring $R = R_n = \mathbb{F}_2[X, Y]/(X^n - 1, Y^n - 1)$. Pressing some buttons means adding a multiple of $i(X, Y) := 1 + X + X^{-1} + Y + Y^{-1}$, where $X^{-1} = X^{n-1}$, $Y^{-1} = Y^{n-1}$. So, n is mad precisely when the ideal $I = (i(X, Y))$ is proper in R, that is, when $i(X, Y)$ is not a unit.

In this formulation, the proof of Lemma 2.2 becomes the observation that $i(X, Y)^2 = i(X^2, Y^2)$, so that $1 + X + X^{-1} + Y + Y^{-1}$ is a unit iff $1 + X^2 + X^{-2} + Y^2 + Y^{-2}$ is.

Proposition 3.1 *Let $\mathbf{F} = \mathbb{F}_q$ be the finite field of order $q = 2^{\phi(n)}$. The number n is mad iff the equation $i(X, Y) = 0$ has a solution in $\mathbf{F}$ consisting of n-th roots of unity.*

Proof. Since squaring is a field automorphism, we may suppose that n is odd. Since $i(X, Y)^2 = i(X^2, Y^2)$ and $2^{\phi(n)} = 1 \pmod n$, we have $i(X, Y)^q = i(X, Y)$, and $i(X, Y)$ is invertible in R iff $i(X, Y)^{q-1} = 1$. If $i(a, b) = 0$ for certain $a, b \in \mathbf{F}$ with $a^n = b^n = 1$, then $i(X, Y)$ is contained in the kernel of the homomorphism $R \to \mathbf{F}$ defined by $f(X, Y) \mapsto f(a, b)$, while 1 is not, so $(i(X, Y))$ is a proper ideal in R. Conversely, if $i(a, b) \neq 0$ for all n-th roots of unity $a, b \in \mathbf{F}$, then the polynomial $f(X, Y) := i(X, Y)^{q-1} - 1$ satisfies $f(a, b) = 0$ for these a, b, and hence $f(X, Y) \in (X^n - 1, Y^n - 1)$, i.e., $f(X, Y) = 0$ in R. □

The following theorem shows that there are infinitely many MAD numbers.

Theorem 3.2 *$2^k - 1$ is mad for all $k \neq 1, 3$.*

Proof. It suffices to show that $1 + X + X^{-1} + Y + Y^{-1} = 0$ has a solution in $\mathbb{F}_q$ for $q = 2^k$, since all nonzero elements of this field are n-th roots of unity for $n = 2^k - 1$. We have to show that the cubic curve $X^2Y + XY^2 + XYZ + XZ^2 + YZ^2 = 0$ has a point over $\mathbb{F}_q$ with $XYZ \neq 0$. This curve is nonsingular, and hence has at least $q + 1 - 2\sqrt{q}$ rational points, of which 4 have $XYZ = 0$, so at least $q - 3 - 2\sqrt{q}$ with $XYZ \neq 0$. For $k \geq 4$ we have $q - 3 - 2\sqrt{q} > 0$. □

Theorem 3.3 *$(2^k-1)/d$ is mad for $(3d)^4 \le 2^k$.*

Proof. Consider the curve $1+X^d+X^{-d}+Y^d+Y^{-d}=0$ over $\mathbb{F}_q$ for $q=2^k$. After multiplication by X^dY^d and homogeneization this becomes $X^{2d}Y^d+X^dY^{2d}+X^dY^dZ^d+X^dZ^{2d}+Y^dZ^{2d}=0$. This curve is singular, but absolutely irreducible, and has at least $q+1-(3d-1)(3d-2)\sqrt{q}$ points, of which $d+3$ have $XYZ=0$, so at least $q-d-2-(3d-1)(3d-2)\sqrt{q}$ points with $XYZ\neq 0$. The hypothesis of the theorem suffices to guarantee that this is positive. □

On the negative side, $73 = 511/7$ and $9709 = (2^{18}-1)/27$ and $3848537 = (2^{30}-1)/279$ are not mad.

Theorem 3.4 *2^k+1 is mad for all $k>0$.*

Proof. The 2^k+1 elements x of $\mathbb{F}_{2^{2k}}$ satisfying $x^{2^k+1}=1$ have $x^{2^k}=x^{-1}$, so that $1+x+x^{-1}+y+y^{-1}=1+\operatorname{tr}x+\operatorname{tr}y$, where $\operatorname{tr}:\mathbb{F}_{2^{2k}}\to\mathbb{F}_{2^k}$ is the trace. Each trace value occurs twice, except for $0=\operatorname{tr}1$, so that the set T of elements of $\mathbb{F}_{2^k}$ of the form $x+x^{-1}$ where $x^{2^k+1}=1$ has size $2^{k-1}+1$. But then the equation $a+b=1$ has a solution in T. □

Lemma 3.5 *The 2^{k-1} nonzero values z in $\mathbb{F}_{2^k}$ of the form $x+x^{-1}$ for some x in $\mathbb{F}_{2^{2k}}$ with $x^{2^k+1}=1$ are precisely the values with $\operatorname{Tr}z^{-1}=1$, where $\operatorname{Tr}:\mathbb{F}_{2^k}\to\mathbb{F}_2$ is the trace.*

Proof. Consider $S=\sum_{i=0}^{k-1}(x+x^{-1})^{2^{k-1}-2^i}$. By Lucas, the expansion of $(x+x^{-1})^{2^{k-1}-2^i}$ contains precisely those terms x^m where $-2^{k-1}<m<2^{k-1}$ and $m\equiv 2^{k-1}-2^i \pmod{2^{i+1}}$. So each m is seen precisely once, and $S=\sum_{j=1}^{2^k-1}x^{2^{k-1}-j}$. For $x^{2^k+1}=1$, $x\neq 1$ and $z=x+x^{-1}$ we find $S+z^{2^{k-1}}=\sum_{j=0}^{2^k}x^{2^{k-1}-j}=0$ and hence $\operatorname{Tr}z^{-1}=\sum_{i=0}^{k-1}z^{-2^i}=z^{-2^{k-1}}S=1$. □

Theorem 3.6 *$(2^k+1)/d$ is mad for $(4d)^4\le 2^k$.*

Proof. Consider the curve $F(X,Y)=1+X^d+X^{-d}+Y^d+Y^{-d}=0$ over $\mathbb{F}_{2^{2k}}$ and seek solutions where X and Y are (2^k+1)-st roots of unity. Since $\{1,X+X^{-1},\dots,X^m+X^{-m}\}$ and $\{(X+X^{-1})^h \mid h=0,1,\dots,m\}$, span the same space, we may rewrite $F(X,Y)$ as a polynomial $G(Z,W)$ of degree d in $Z=X+X^{-1}$ and $W=Y+Y^{-1}$ and seek solutions over $\mathbb{F}_{2^k}$ where Z and W have inverses of trace 1.

Now the elements of $\mathbb{F}_{2^k}$ of trace 1 have the form u^2+u+a, where a is a fixed element of trace 1. So, we can substitute $Z=1/(U^2+U+a)$ and $W=1/(V^2+V+a)$ and find a polynomial $H(U,V)=Z^{-d}W^{-d}G(Z,W)$ of degree $4d$ in U and V. The result follows. □

On the negative side, $43=129/3$ and $241=4097/17$ and $4033=(2^{18}+1)/65$ are not mad.

4 2-order

Examples seem to show that MAD numbers have small 2-order. We give some resuls in this direction.

For odd n, let $\mathrm{ord}(n)$ denote the multiplicative order of 2 mod n, and let $\mathrm{pmord}(n)$ denote the smallest $k > 0$ with $2^k = \pm 1 \pmod{n}$. (So $\mathrm{pmord}(n) = \mathrm{ord}(n)$ or $\mathrm{pmord}(n) = \mathrm{ord}(n)/2$. We are in the first case for $n = 15$, $\mathrm{ord}(n) = 4$.)

Lemma 4.1 *Let n be odd, and let g be a primitive n-th root of unity (in a suitable extension of $\mathbb{F}_2$). Then the minimal polynomial of g over $\mathbb{F}_2$ has degree $\mathrm{ord}(n)$. Any polynomial with roots both g and g^{-1} has degree at least $2\,\mathrm{pmord}(n)$.*

Proof. The conjugates of g are the powers g^{2^m}, and there are $\mathrm{ord}(n)$ of them. If these are also the conjugates of g^{-1}, then $\mathrm{pmord}(n) = \mathrm{ord}(n)/2$. □

Theorem 4.2 *If p is an odd prime, and p is mad, then*

$$\mathrm{pmord}(p) \leq \sqrt{p}.$$

Proof. Let $i(x, y) = 0$ for some x and y that are p-th roots of unity. In terms of a fixed primitive p-th root of unity g we have for certain a and b:

$$1 + g^{-a} + g^a + g^{-b} + g^b = 0.$$

Let Λ be the sublattice of $\mathbb{Z} \times \mathbb{Z}$ spanned by the vectors $(a, b), (p, 0), (0, p)$. Since Λ has index p, a fundamental domain for Λ has area p. By Minkowski's theorem Λ has a nonzero point (c, d) in the bounded symmetric convex set $K = \{(x, y) \mid |x|, |y| \leq \sqrt{p}\}$. If $(c, d) = s(a, b) + t(p, 0) + u(0, p)$, then $s \neq 0 \pmod{p}$. Let $rs = 1 \pmod{p}$ and put $h = g^r$, so that $g = h^s$. Now

$$1 + h^{-c} + h^c + h^{-d} + h^d = 0.$$

We see that h and h^{-1} satisfy the same equation of degree $2\max(|c|, |d|) \leq 2\sqrt{p}$ and the above lemma yields the required inequality. □

5 Computer search

In this section we describe how the algebraic condition for a number n to be mad can be translated into a reasonably fast algorithm to test for madness.

Define polynomials $f_m(U)$ in $\mathbb{F}_2[U]$ by

$$f_0(U) = 0,\ f_1(U) = 1,\ f_m(U) = U\, f_{m-1}(U) + f_{m-2}(U) \text{ for } m > 1.$$

Theorem 5.1 *Let $g_n(U) = U\, f_n(U)$. The number n is mad if and only if*

$$\gcd(g_n(U), g_n(U + 1)) \neq 1.$$

Proof. Note that $g_n(X + X^{-1}) = X^n + X^{-n}$. The number n is mad if and only if $1 + X + X^{-1} + Y + Y^{-1} = 0$ has a solution in n-th roots of unity. Put $U = X + X^{-1}$ and $Y = Y + Y^{-1}$. Then n is mad if and only if $1 + U + V = 0$ has a solution in roots of g_n. □

Theorem 5.2 *Let $h_m(U) = g_m(U) + g_{m+1}(U)$. The number $n = 2m + 1$ is mad if and only if*

$$\gcd(h_m(U), h_m(U + 1)) \neq 1.$$

Proof. Note that $h_m(X + X^{-1}) = X^{m+1} + X^m + X^{-m} + X^{-m-1} = (X^n + 1)(X + 1)X^{-m-1}$. The number $n = 2m+1$ is mad if and only if $1+X+X^{-1}+Y+Y^{-1} = 0$ has a solution in n-th roots of unity. Put $U = X + X^{-1}$ and $V = Y + Y^{-1}$. Then n is mad if and only if $1 + U + V = 0$ has a solution in roots of h_m. □

Using this condition we used the Mathematica package to test some small numbers, and the first interesting MAD number (that is not of the form $2^k \pm 1$ was found: $683 = (2^{11} + 1)/3$. Motivated by this we wrote a little C program to check all numbers up to 10^5 (this took approximately 100 hours of CPU-time) and all numbers $n < 10^6$ with $\mathrm{ord}(n) \leq 100$. The fact that all numbers that turned out to be MAD had 2-order at most 30 indicated that the list is probably complete. Later Andries tested his new computer and checked all n up to 10^7, and those of $\mathrm{pmord}(n) \leq 200$ up to 10^9, finding a total of 62 mad numbers, all with $\mathrm{pmord}(n) \leq 54$.

6 Table

Table 1 below gives all known MAD numbers less than 10^9. It is complete up to 10^7 and also contains all MAD numbers n with $n < 10^9$ and $\mathrm{pmord}(n) < 200$.

3	5	17	31	127
257	511	683	2047	2731
3277	3641	8191	43691	52429
61681	65537	85489	131071	174763
178481	233017	253241	256999	486737
524287	704093	838861	1016801	1082401
1657009	1838599	1965379	2304167	2796203
3033169	3303821	3605429	3705353	6700417
8727391	9335617	13788017	15790321	19173961
21225581	24214051	25080101	25781083	53353631
102964687	120296677	164511353	207207011	240068041
256957153	464955857	598781009	616318177	715827883
905040953	993089953			

Table 1: The 62 known MAD numbers less than 10^9

7 Historical remarks

Most of the above was found by Aart Blokhuis in 1994 or 1995 and lived in old preprints and on web pages. This old material was revived in 2015 when the table was extended.