Proof of the Alon-Tarsi Conjecture for $n = 2^r p$

Arthur A. Drisko

National Security Agency
Fort George G. Meade, MD 20755
arthur.drisko.td.90@aya.yale.edu

Submitted: April 10, 1998; Accepted: May 10, 1998.

Abstract

The Alon-Tarsi conjecture states that for even n, the number of even latin squares of order n differs from the number of odd latin squares of order n. Zappa [6] found a generalization of this conjecture which makes sense for odd orders. In this note we prove this extended Alon-Tarsi conjecture for prime orders p. By results of Drisko [2] and Zappa [6], this implies that both conjectures are true for any n of the form $2^r p$ with p prime.

1 Introduction

A *latin square* L of order n is an $n \times n$ matrix whose rows and columns are permutations of n symbols, say $0, 1, \ldots, n-1$. Rows and columns will also be indexed by $0, 1, \ldots, n-1$. The *sign* $\operatorname{sgn}(L)$ of L is the product of the signs (as permutations) of the rows and columns of L. L is *even*, respectively *odd*, if $\operatorname{sgn}(L)$ is $+1$, respectively -1. A *fixed diagonal* latin square has all diagonal entries equal to 0.

We denote the set of all latin squares of order n by $\mathrm{LS}(n)$ and the set of all fixed diagonal latin squares of order n by $\mathrm{FDLS}(n)$. We denote the numbers of even, odd, fixed diagonal even, and fixed diagonal odd latin squares of order n by $\mathrm{els}(n)$, $\mathrm{ols}(n)$, $\mathrm{fdels}(n)$, and $\mathrm{fdols}(n)$, respectively.

If $n \neq 1$ is odd, then switching two rows of a latin square alters its sign, so $\mathrm{els}(n) = \mathrm{ols}(n)$. On the other hand, Alon and Tarsi [1] conjectured:

Conjecture 1 (Alon-Tarsi) *If n is even then* $\mathrm{els}(n) \neq \mathrm{ols}(n)$.

Equivalently, the sum of the signs of all $L \in \mathrm{LS}(n)$ is nonzero. This conjecture is related to several other conjectures in combinatorics and linear algebra [3, 5].

Zappa was able to generalize this conjecture to the odd case by defining the Alon-Tarsi constant

$$\mathrm{AT}(n) = \frac{\mathrm{fdels}(n) - \mathrm{fdols}(n)}{(n-1)!}. \tag{1}$$

MR Subject Classification (1991): 05B15, 05E20, 05A15

Since any latin square can be transformed into a fixed diagonal latin square by a permutation of rows, and since permuting rows does not change the sign of a latin square of even order, we have

$$\mathrm{els}(n) - \mathrm{ols}(n) = \begin{cases} n!(n-1)!\,\mathrm{AT}(n) & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd.} \end{cases} \tag{2}$$

Only a few values of $\mathrm{AT}(n)$ are known [4, 6]:

n	2	3	4	5	6	7	8
$\mathrm{AT}(n)$	1	-1	4	-24	$2,304$	$368,640$	$6,210,846,720$

Zappa conjectured this generalization of the Alon-Tarsi conjecture:

Conjecture 2 (Extended Alon-Tarsi) *For every positive integer n,*

$$\mathrm{AT}(n) \neq 0.$$

Aside from the table of known values, we have the following information about $\mathrm{AT}(n)$ [2, 6]:

Theorem 1 (Drisko) *If p is an odd prime, then*

$$\mathrm{els}(p+1) - \mathrm{ols}(p+1) \equiv (-1)^{\frac{p+1}{2}} p^2 \pmod{p^3}.$$

This implies that $\mathrm{AT}(p+1) \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$, by (2).

Theorem 2 (Zappa) *If n is even, then*

$$\mathrm{AT}(n) \neq 0 \Longrightarrow \mathrm{AT}(2n) \neq 0,$$

and if n is odd, then

$$\mathrm{AT}(n) \neq 0 \text{ and } \mathrm{AT}(n+1) \neq 0 \Longrightarrow \mathrm{AT}(2n) \neq 0.$$

Together, these imply the truth of the Alon-Tarsi conjecture for $n = 2^r(p+1)$ for any $r \geq 0$ and any odd prime p (and, by the table of known values, for $p = 2$ also). Our goal here is to prove that $\mathrm{AT}(p) \neq 0$ for all primes p. This then implies that the extended Alon-Tarsi conjecture is true for all $n = 2^r p$, where $r \geq 0$ and p is any prime.

2 The Result

The approach is the same as in [2]. Let S_n be the symmetric group on $\{0, 1, \ldots, n-1\}$ and let $\mathfrak{I}_n = S_n \times S_n \times S_n$. This group acts on the set $\mathrm{LS}(n)$ of latin squares of order n by permuting the rows, columns, and symbols, and is called the *isotopy group*.

Let G be any subgroup of $\mathfrak{I}_n$. We shall call two latin squares L, M of order n *G-isotopic* if there exists $g \in G$ such that $Lg = M$. The orbit LG of L under G is the *G-isotopy class* of L. The *G-autotopism group* $\mathfrak{A}_G(L)$ of L is the stabilizer of L in G. Clearly

$$|G| = |LG||\mathfrak{A}_G(L)| \tag{3}$$

for any $G < \mathfrak{I}_n$ and any latin square L of order n.

We need one well-known lemma (see [2] or [4]).

Lemma 3 *Let L be any latin square of order n and $g = (\alpha, \beta, \gamma) \in \mathfrak{I}_n$. Then*

$$\mathrm{sgn}(Lg) = \mathrm{sgn}(\alpha)^n \mathrm{sgn}(\beta)^n \mathrm{sgn}(\gamma)^{2n} \mathrm{sgn}(L) = \mathrm{sgn}(\alpha)^n \mathrm{sgn}(\beta)^n \mathrm{sgn}(L).$$

We are now ready for our main result.

Theorem 4 *Let p be an odd prime. Then*

$$\mathrm{AT}(p) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}. \tag{4}$$

Proof. Let

$$G = \{(\sigma, \sigma, \tau) : \sigma, \tau \in S_p, 0\tau = 0\}. \tag{5}$$

G acts on FDLS(p). By Lemma 3, $\mathrm{sgn}(Lg) = \mathrm{sgn}(L)$ for any L of order p and any $g \in G$. Let R be any set of representatives of the orbits of G in FDLS(p), and let S be a set of representatives of those orbits of size not divisible by p. Then

$$\begin{aligned}
\mathrm{fdels}(p) - \mathrm{fdols}(p) &= \sum_{L \in \mathrm{FDLS}(p)} \mathrm{sgn}(L), && (6)\\
&= \sum_{L \in R} |LG| \mathrm{sgn}(L), && (7)\\
&\equiv \sum_{L \in S} |LG| \mathrm{sgn}(L) \pmod{p}. && (8)
\end{aligned}$$

Since $|G| = p!(p-1)!$, $|LG|$ is not divisible by p if and only if p divides $|\mathfrak{A}_G(L)|$.

Suppose p divides $|\mathfrak{A}_G(L)|$ for some L. Then there is some G-autotopism $g = (\sigma, \sigma, \tau)$ of L of order p. Since $\tau \in S_p$ fixes 0, $\tau^p = e$ implies that $\tau = e$. Since g is not the identity, $\sigma^p = e$ implies that σ is a p-cycle, so that $\rho^{-1}\sigma\rho = (0\ 1\ \cdots\ p-1)$ for some $\rho \in S_p$. Then $M = L(\rho, \rho, e)$ is G-isotopic to L and has G-autotopism $((0\ 1\ \cdots\ p-1), (0\ 1\ \cdots\ p-1), e)$. It is clear that such an M must have constant diagonals (that is, $M_{i,j} = M_{i+1,j+1}$ for all i, j, taken mod p). But then there is some $\mu \in S_p$, fixing 0, such that $N = M(e, e, \mu)$, where N is the square given by $N_{i,j} = i - j \pmod{p}$. Hence any L with G-autotopism group divisible by p is G-isotopic to N, so there is only one isotopy class in the sum (8), and its size is not divisible by p. Therefore,

$$\mathrm{fdels}(p) - \mathrm{fdols}(p) \equiv |NG| \mathrm{sgn}(N) \pmod{p}. \tag{9}$$

Now, the columns of N, as permutations, are powers of the p-cycle $\phi = (0\,1\ \cdots\ p{-}1)$, so they all have positive sign. Each row, as a permutation, consists of one fixed point and $(p-1)/2$ transpositions, and there are an odd number of rows, so

$$\mathrm{sgn}(N) = (-1)^{\frac{p-1}{2}}. \tag{10}$$

To determine $|NG|$, let $g = (\sigma, \sigma, \tau) \in \mathfrak{A}_G(N)$. We know that $h = (\phi, \phi, e) \in \mathfrak{A}_G(N)$, so for some k, $gh^k = (\sigma\phi^k, \sigma\phi^k, \tau) \in \mathfrak{A}_G(N)$ and $\sigma\phi^k$ fixes 0. Then

$$\begin{aligned} i\tau &= N_{i,0}\tau \\ &= N_{i\sigma\phi^k, 0\sigma\phi^k} \\ &= N_{i\sigma\phi^k, 0} \\ &= i\sigma\phi^k \end{aligned}$$

for all i, so $gh^k = (\tau, \tau, \tau)$. But then for all $i, j \in Z_p$, the cyclic group of order p, we have

$$\begin{aligned} (i-j)\tau &= N_{i,j}\tau \\ &= N_{i\tau, j\tau} \\ &= (i\tau - j\tau), \end{aligned}$$

so τ must be an automorphism of Z_p. Hence every G-autotopism of N is an automorphism of Z_p times a power of h and we have

$$|\mathfrak{A}_G(N)| = p|\mathrm{Aut}(Z_p)| = p(p-1), \tag{11}$$

and combining this with (3), we get

$$\begin{aligned} |NG| &= \frac{p!(p-1)!}{p(p-1)} \\ &= (p-1)!(p-2)!\,. \end{aligned} \tag{12}$$

Finally, combining (9), (10), and (12), we have

$$\begin{aligned} \mathrm{AT}(p) &= \frac{\mathrm{fdels}(p) - \mathrm{fdols}(p)}{(p-1)!} \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\frac{(p-1)!(p-2)!}{(p-1)!}\right] \pmod p \\ &\equiv (-1)^{\frac{p-1}{2}} (p-2)! \pmod p \\ &\equiv (-1)^{\frac{p-1}{2}} \pmod p, \end{aligned} \tag{13}$$

since $(p-2)! \equiv 1 \pmod p$, by Wilson's theorem. □

Let us record the known cases of the extended Alon-Tarsi conjecture as

Corollary 5 *Let p be any prime and r any nonnegative integer. Then*

$$\mathrm{AT}(2^r p) \neq 0 \text{ and } \mathrm{AT}(2^r(p+1)) \neq 0.$$

Although the truth of the extended conjecture is still unknown for $n = 9$, the first *even* value of n which is not of the form given in Corollary 5 is 50, whereas the previous first unknown case of the original Alon-Tarsi conjecture was $n = 22$.

References

[1] N. Alon and M. Tarsi, Coloring and orientations of graphs, *Combinatorica* **12** (1992), 125–143

[2] A. A. Drisko, On the number of even and odd latin squares of order $p+1$, *Adv. Math.* **128** (1997), 20–35.

[3] R. Huang and G.-C. Rota, On the relations of various conjectures on Latin squares and straightening coefficients, *Discrete Math.* **128** (1994), 237–245.

[4] J. C. M. Janssen, On even and odd latin squares, *J. Combin. Theory Ser. A* **69** (1995), 173–181.

[5] S. Onn, A colorful determinantal identity, a conjecture of Rota, and latin squares, *Amer. Math. Monthly* **104** (1997), 156–159.

[6] P. Zappa, The Cayley determinant of the determinant tensor and the Alon-Tarsi conjecture, *Adv. Appl. Math.* **19** (1997), 31–44.