SIAM J. DISCRETE MATH.
Vol. 24, No. 2, pp. 394–399

THE CONJECTURES OF ALON–TARSI AND ROTA IN DIMENSION PRIME MINUS ONE*

DAVID G. GLYNN†

Abstract. A formula for Glynn's hyperdeterminant $\det_p$ (p prime) of a square matrix shows that the number of ways to decompose any integral doubly stochastic matrix with row and column sums $p-1$ into $p-1$ permutation matrices with even product, minus the number of ways with odd product, is 1 (mod p). It follows that the number of even Latin squares of order $p-1$ is not equal to the number of odd Latin squares of that order. Thus Rota's basis conjecture is true for a vector space of dimension $p-1$ over any field of characteristic zero or p, and all other characteristics except possibly a finite number. It is also shown where there is a mistake in a published proof that claimed to multiply the known dimensions by powers of two, and that also claimed that the number of even Latin squares is greater than the number of odd Latin squares. Now, 26 is the smallest unknown case where Rota's basis conjecture for vector spaces of even dimension over a field is unsolved.

Key words. basis conjecture, doubly stochastic matrix, Latin square, permutation, hyperdeterminant, Cayley, Rota, vector space

AMS subject classifications. 05B15, 05B20, 05B75, 05C20, 11A41, 15A03, 15A15, 15A72, 15B51, 51E20

DOI. 10.1137/090773751

1. Rota's basis conjecture.

Rota's basis conjecture for matroids is the following; see [14].

CONJECTURE 1.1. *Consider any matroid N of rank n. Let $A = (a_{ij})$ be an $n \times n$ matrix such that every element a_{ij} is a point of N (an element of rank one) and each row of A is a basis of N. Then the elements in each row of A can be permuted so that in the resulting $n \times n$ matrix every column also forms a basis for N.*

This has been verified for $n \leq 3$; see [5]. It is also true for linear matroids of rank $p+1$ (p prime) over fields of all characteristics, except possibly a finite number of prime characteristics; see [8]. There has been a great deal of recent interest in this conjecture as verified by the following papers: [1, 3, 5, 6, 8, 9, 10, 11, 15, 16, 17, 18, 19].

Now let us state the conjecture due to *Alon–Tarsi* [2]. It is equivalent to another of Huang–White; see [15].

CONJECTURE 1.2. *The number of Latin squares of a given even order of even parity is not equal to the number of Latin squares of that order of odd parity.*

The definitions for the parities are well known, but we repeat them in section 2 using a nonstandard explanation. From [12, 14, 16], if the Alon–Tarsi conjecture is true for a certain even n, then Rota's basis conjecture for fields of characteristic 0 and dimension n is true, and this holds also for fields of almost all prime characteristics.

In [19] there are some results which state that if the Alon–Tarsi conjecture is true for even m, then it is true for all $m.2^i, i \geq 0$, and if an extended Alon–Tarsi conjecture is true for odd m (where the Latin squares are assumed to have a constant diagonal) and Alon–Tarsi is true for even $m+1$, then Alon–Tarsi is true for $m.2^i$, $i > 0$. However, there is a misunderstanding on page 38, in section 3 after equation (10), involving

*Received by the editors October 13, 2009; accepted for publication (in revised form) January 31, 2010; published electronically April 14, 2010.
http://www.siam.org/journals/sidma/24-2/77375.html

†CSEM, Flinders University, P.O. Box 2100, Adelaide, South Australia 5001, Australia (davidg@csem.flinders.edu.au, david.glynn@csem.flinders.edu.au, dglynn@me.com).

the numerical difference $2n+1-i_j$ and the set-theoretic complement $I_{2n}-J_j$. The first is not necessarily in the second if i_j is in J_j. So the main results of that paper come into doubt. This has been acknowledged by the author of [19] in a personal communication. There are still some redeeming points in the paper which repay reading, including an explanation of more properties of Cayley's hyperdeterminant $\det_0$, first defined in [4].

The next section explains a method for calculating the various invariant parities of a Latin square of even order. The final section shows that the Alon–Tarsi conjecture is true for Latin squares of orders prime minus one, thus implying Rota's basis conjecture for linear matroids of these dimensions over fields of almost all characteristics.

2. Latin squares. Consider a *Latin square* $L=(l_{ij})$ of *even* order m, having symbols from the set $M:=\{1,\dots,m\}$. See [7] for the definitions. It has various invariant *parities* that do not change under permutations of the rows, permutations of the columns, and renaming the elements of the square, i.e., *isotopies*.

A way to obtain these parities is as follows. From L construct an *orthogonal array*, which is an $m^2\times 3$ array H with elements from M, with the rows of H being in bijective correspondence with the m^2 positions in L. In a row of H put i,j,k if the corresponding position of L has $l_{i,j}=k$. Since L is a Latin square, every pair of columns, (a,b) of H are similar: the rows of the corresponding $m^2\times 2$ submatrix are all distinct and make up all the pairs in $M\times M$.

Given a pair of distinct columns (a,b) of H, define an associated parity in $\mathbb{Z}_2$:

$$\rho(a,b):=\Sigma_{1\le i<j\le m^2}\ \delta(h_{i,a}-h_{j,a}).S(h_{i,b}-h_{j,b}) \pmod 2,$$

where S is the Heaviside unit step function defined by

$$S(x):=\begin{cases}0, & x\le 0,\\ 1, & x>0,\end{cases}$$

and where δ is its "derivative" Dirac unit impulse function defined by

$$\delta(x):=\begin{cases}0, & x\ne 0,\\ 1, & x=0.\end{cases}$$

A directed graph $G(H)$ is defined as having three vertices in correspondence with the columns of H such that if (a,b) is an ordered pair of columns of H, then there is a directed edge from a to b in G if and only if $\rho(a,b)=1$.

While $G(H)$ depends on the ordering of the rows of H, there are only $2^3=8$ possible directed graphs that come from the same Latin square, related by complementing the set of out-edges from a subset of the three vertices.

We can define the various *parities* of the Latin square and see how they are related. Let the columns (in order) of H be a,b,c: the elements in the first column a of H correspond to the rows of L, the elements in the second column b of H to the columns of L, and the elements in the third column c of H to the symbols in L.

The *row, column, or symbol parity* of L is *even* if there is an even number of edges going out from a,b, or c in $G(H)$, respectively, and is *odd* otherwise. Use the notation rowpar(L), colpar(L), sympar(L), respectively, for these parities.

Another method for finding these parities is to find the signs of the products of the permutations in the rows, columns, and symbols, respectively, in L. However, the above method generalizes to orthogonal arrays of even order with larger numbers of columns.

A result of Richard Wilson is the following.

THEOREM 2.1. *The total number of directed edges in the graph G of the Latin square L of order m is even if $m \equiv 0 \pmod 4$, while it is odd if $m \equiv 2 \pmod 4$, i.e., for the Latin square* $\mathrm{rowpar}(L) + \mathrm{colpar}(L) + \mathrm{sympar}(L) \equiv m/2 \pmod 2$.

Proof. There is a proof in [15] which is numerical but fairly opaque. Here is another proof. First, the number E of directed edges modulo two in G is $\Sigma_{a \neq b}\ \rho(a,b)$ over the six pairs (a,b) of distinct columns of the orthogonal array H. To count this it is perhaps easiest to associate with H a $\binom{q^2}{2} \times 3$ array K, where the rows of K correspond to unordered pairs of rows of H, and the columns of K are in correspondence with the columns of H. In a given row r of K corresponding to rows i and j of H, $i < j$, consider a given column c. Put a symbol s into $k_{r,c}$ if $h_{i,c} = h_{j,c}$, i.e., $\delta(h_{i,c} - h_{j,c}) = 1$. Otherwise, if $h_{i,c} < h_{j,c}$, i.e., $S(h_{i,c} - h_{j,c}) = 0$, put $k_{r,c} = d$, and lastly, if $h_{i,c} > h_{j,c}$, i.e., $S(h_{i,c} - h_{j,c}) = 1$, put $k_{r,c} = u$. Note that s stands for "same," d for "down," and u for "up." Hence E is the number of times (modulo two) that s and u appear in the same row of K. We have to count the number of rows with s, u, d appearing in some order, since any other possible rows have an even number of s, u unordered pairs. However, now we can count the u, d unordered pairs in each row (modulo two as always). This is the same as counting E, since rows without an s such as u, u, u or u, d, u and so on also have an even number of u, d unordered pairs. (There are no rows such as s, s, u.) But we can count the u, d unordered pairs in the rows for each unordered pair of columns of K as follows. Consider the "standard" pair of columns of H with the lexicographic order: this contains $1, \ldots, 1, 2, \ldots, 2, \ldots, m, \ldots, m$ in the first column and $1, 2, \ldots, m, 1, 2, \ldots, m, \ldots, 1, 2, \ldots, m$ in the second column. It is easy to see that the corresponding two columns of K have no u's in the first column, and so no rows of type u, d, but there are $\binom{m}{2}^2$ rows which are d, u. If we transpose two consecutive rows of H and consider any two columns, a pair u, d in the corresponding single row of K is transformed into a pair d, u, and vice versa. So the total number of unordered pairs u, d in any two columns of K is an invariant, independent of the ordering of the rows of H. It is always $\binom{m}{2}^2$. Since there are three unordered pairs of columns of H or K, this shows that $E \equiv 3\binom{m}{2}^2 \pmod 2$, which is $m/2 \pmod 2$, since m is even. ∎

By using complementations of the out-edges at various vertices of G, it is seen that there are two basic kinds of Latin square when $m \equiv 2 \pmod 4$, with invariant graphs G being a cyclic tournament or an acyclic tournament. When $m \equiv 0 \pmod 4$, there are also two basic types: one corresponding to the empty graph and the other to simple graph with one undirected edge (two superposed directed edges). However, this partitioning of the Latin squares into two types is not the same as that given by the *parity*, $\mathrm{parity}(L)$, of the Latin square L; see [15].

DEFINITION 2.2. $\mathrm{parity}(L) \equiv \mathrm{rowpar}(L) + \mathrm{colpar}(L) \pmod 2$. *A Latin square of even order m is said to be* even *if* $\mathrm{parity}(L) \equiv 0 \pmod 2$, *and it is said to be* odd *if* $\mathrm{parity}(L) \equiv 1 \pmod 2$.

From Theorem 2.1 we have the following.

COROLLARY 2.3. *For any Latin square of even order m,*

$$\mathrm{parity}(L) \equiv \mathrm{sympar}(L) + m/2 \pmod 2.$$

The *conjugates* of a Latin square are obtained by permuting the roles of the rows, columns, and symbols. Thus there are six conjugacy classes giving orthogonal arrays that are related by permuting the three columns. The invariant graphs or tournaments above will be the same and independent of the conjugate that is taken. However, the

parity of the Latin square depends on the row/column pair, and so the parity can be different for other conjugates.

The following result connecting the Alon–Tarsi conjecture to Rota's basis conjecture for linear matroids of rank m (over fields) or, equivalently, for vector spaces of rank m over fields of characteristic zero, is found in [12, 14, 16]. A *reduced* Latin square has the first row (or column) in standard order. The number of reduced Latin squares (of even or odd type) is therefore the number of Latin squares of that type divided by $m!$.

THEOREM 2.4. *If the number n_e of even reduced Latin squares of order m (even) is not equal to the number n_o of odd reduced Latin squares of that order, then Rota's basis conjecture is true for vector spaces of rank m over a field. (Necessarily, the characteristic of the field has to be zero or bigger than m, not dividing $m!$, and it cannot divide $n_e - n_o$. This excludes a finite number of characteristics if $n_e - n_o \neq 0$.)*

In the next section we can apply this to orders m that are a prime minus one.

3. The decomposition of doubly stochastic matrices. Some definitions and properties are needed from [13]. A *hypercube* of dimension m^n (where m is the side length and n is a positive integer) has mn slices, which are all m^{n-1} hypercubes. Fixing one of the n directions, there are m slices obtained by fixing an index in that direction.

Given a hypercube H over a field of prime characteristic p of dimension m^n, the modular hyperdeterminant $\det_p(H)$ (times $(-1)^m$) is the sum over all monomials in the elements of H such that the monomial has its exponents summing to $p-1$ on each slice. There is also a division by the product of the factorials of the exponents involved with each monomial. Thus $\det_p$ is a polynomial of degree $m(p-1)$ in m^n variables, and the monomials have coefficients that are in $GF(p)$.

An alternative way (not previously published) to calculate this formula is to consider $m(p-1) \times n$ "exponent" tables T made up of integers from the set $\{0, \ldots, p-1\}$. One column (usually the first) is always the same: $1, \ldots, 1, \ldots, m, \ldots, m$, with each i $(1 \leq i \leq m)$ repeated $p-1$ times. The other $n-1$ columns are permutations of this column. This implies that there are $\binom{m(p-1)}{p-1,\ldots,p-1}$ possible columns, and therefore $\binom{m(p-1)}{p-1,\ldots,p-1}^{n-1}$ tables T with the same fixed column.

Each such table corresponds to a monomial in $\det_p$ of degree $m(p-1)$ in the m^n variables: any row of T is an index for a particular element of H, and these $m(p-1)$ elements are multiplied. Note that two different tables T and T' can give rise to the same monomial, and this happens when T' is obtained by permuting rows of T. It can be confirmed that this is the same formula as given by the first method, up to the factor $(-1)^m$.

Note that this alternative method for constructing $\det_p$ is very similar to the original method of Cayley from 1843 for constructing $\det_0$. He used an $m \times n$ table and also fixed a column. A difference there, however, was that the columns were permutations with a certain sign, and the product of the signs of the columns gave the multiplying factor for the corresponding monomial. In that case, two nonidentical tables could not give the same monomial, since permuting rows of a table would also permute the rows of the fixed column $1, \ldots, m$. For characteristic two fields, $\det_2 = \det_0$ holds. In [13] the following formula is shown.

THEOREM 3.1. *If A is an $m \times m$ matrix over a field of characteristic p, then*

$$\det_p(A) = \det(A^{p-1}).$$

By the Cauchy–Binet multiplicative property of the determinant we can write $\det(A^{p-1})$ as a product of the $p-1$ determinants $\det(A)$. Using the standard formula for $\det(A)$ as a sum of $m!$ monomials, with plus or minus signs depending upon whether the monomial comes from an even or an odd permutation, respectively, we can also write $\det(A)^{p-1}$ as a sum of monomials. Each of these is a product of the elements a_{ij} of A with certain exponents e_{ij} having $0 \leq e_{ij} \leq p-1$, and there is an integer coefficient for each monomial. The exponents e_{ij} form an $m \times m$ matrix E that is "doubly stochastic": the row and column sums of E are all $p-1$. The integer coefficient for the monomial can be calculated by finding all possible ways to write E as an ordered sum of $p-1$ permutation matrices of side m. If there is an odd number of odd permutations in this sum, then the contribution to the integer coefficient of the monomial is -1; otherwise it is $+1$.

The above formula for $\det_p(A)$ implies that, modulo p, the integer coefficient for each monomial with a doubly stochastic exponent matrix E is nonzero modulo p, and so it is nonzero as an integer. In the special case where $m = p-1$, consider the exponent matrix $E = J$, the $(p-1) \times (p-1)$ doubly stochastic matrix of all ones. Each way of writing E as an ordered sum of $p-1$ permutation matrices of side $p-1$ corresponds to a Latin square of side $p-1$, and there is a bijective correspondence between these ways and the Latin squares because every symbol in the Latin square occurs as a permutation matrix. A Latin square with an odd number of permutation matrices (where the symbols are the same) that are odd has odd symbol parity; see section 2. From Corollary 2.3, for a Latin square L of even order $p-1$, $\text{parity}(L) \equiv \text{sympar}(L) + (p-1)/2 \pmod 2$. Thus, the formula for $\det_p$ implies the following.

THEOREM 3.2. *For any odd prime p, the number of even Latin squares of order $p-1$ minus the number of odd Latin squares of that order is $(-1)^{(p-1)/2}$ modulo p.*

By the results here we have shown the following.

THEOREM 3.3. *Rota's basis conjecture is true for vector spaces of dimensions $p-1$, where p is a prime, and the characteristic of the base field is zero or p, or any other characteristics, possibly excluding a finite number of them.*

In [8] a similar theorem has been shown for $p+1$. Now $26 = 5^2 + 1 = 3^3 - 1$ is neither a prime plus one nor a prime minus one. The remaining even numbers less than 26 are $2 = 3-1$, $4 = 3+1 = 5-1$, $6 = 5+1 = 7-1$, $8 = 7+1$, $10 = 11-1$, $12 = 11+1 = 13-1$, $14 = 13+1$, $16 = 17-1$, $18 = 17+1 = 19-1$, $20 = 19+1$, $22 = 23-1$, $24 = 23+1$. Thus we have the following.

COROLLARY 3.4. *The smallest unsolved case of even order for the Alon–Tarsi conjecture (and for Rota's basis conjecture for characteristic zero fields) is* 26.

REFERENCES

[1] R. AHARONI AND E. BERGER, *The intersection of a matroid and a simplicial complex*, Trans. Amer. Math. Soc., 358 (2006), pp. 4895–4917.

[2] N. ALON AND M. TARSI, *Colorings and orientations of graphs*, Combinatorica, 12 (1992), pp. 125–134.

[3] E. F. BESCHLER, D. A. BUCHSBAUM, J. T. SCHWARTZ, R. P. STANLEY, B. D. TAYLOR, AND M. WATERMAN, *Gian-Carlo Rota* (1932–1999), Notices Amer. Math. Soc., 47 (2000), pp. 203–216.

[4] A. CAYLEY, *On the theory of determinants*, Camb. Phil. Soc. Trans., VIII (1849), pp. 1–16. (The paper was actually presented at a meeting of the society in 1843.)

[5] W. CHAN, *An exchange property of matroid*, Discrete Math., 146 (1995), pp. 299–302.

[6] T. Y. CHOW, *Reduction of Rota's basis conjecture to a problem on three bases*, SIAM J. Discrete Math., 23 (2009), pp. 369–371.

[7] J. Denes and A. D. Keedwell, *Latin Squares and Their Applications*, English Universities Press, London, 1974.
[8] A. A. Drisko, *On the number of even and odd Latin squares of order $p+1$*, Adv. Math., 128 (1997), pp. 20–35.
[9] A. A. Drisko, *Proof of the Alon–Tarsi conjecture for $n = 2^r p$*, Electron. J. Combin., 5 (1998), research paper 28 (electronic).
[10] J. Geelen and P. J. Humphries, *Rota's basis conjecture for paving matroids*, SIAM J. Discrete Math., 20 (2006), pp. 1042–1045.
[11] J. Geelen and K. Webb, *On Rota's basis conjecture*, SIAM J. Discrete Math., 21 (2007), pp. 802–804.
[12] F. Gherardelli, *Osservazioni sugli iperdeterminanti*, Istit. Lombardo Accad. Sci. Lett. Rend. A, 127 (1993), pp. 107–113.
[13] D. G. Glynn, *The modular counterparts of Cayley's hyperdeterminants*, Bull. Austral. Math. Soc., 57 (1998), pp. 479–492.
[14] R. Huang and G.-C. Rota, *On the relations of various conjectures on Latin squares and straightening coefficients*, Discrete Math., 128 (1994), pp. 225–236.
[15] J. C. M. Janssen, *On even and odd Latin squares*, J. Combin. Theory Ser. A, 69 (1995), pp. 173–181.
[16] S. Onn, *A colorful determinantal identity, a conjecture of Rota, and Latin squares*, Amer. Math. Monthly, 104 (1997), pp. 156–159.
[17] V. Ponomarenko, *Reduction of jump systems*, Houston J. Math., 30 (2004), pp. 27–33.
[18] M. Wild, *On Rota's problem about n bases in a rank n matroid*, Adv. Math., 108 (1994), pp. 336–345.
[19] P. Zappa, *The Cayley determinant of the determinant tensor and the Alon–Tarsi conjecture*, Adv. Appl. Math., 19 (1997), pp. 31–44.