Brad Rodgers
rbrad@umich.edu

Dear Professor Zeilberger,

I want to record the main points of a proof of Saffari's conjecture, although written down somewhat hastily. The method is different from yours. Almost certainly there are a few typographical errors in the exposition below, but I believe the mathematics is correct. (It goes without saying that this proof deserves a more thorough write-up to be more certain of this.)

We recall the inductive definition of Shapiro polynomials: $P_0(z) = Q_0(z) = 1$ and

$$P_{k+1}(z) = P_k(z) + z^{2^k} Q_k(z),$$
$$Q_{k+1}(z) = P_k(z) - z^{2^k} Q_k(z)$$

so that

$$\begin{pmatrix} P_k(z) \\ Q_k(z) \end{pmatrix} = \begin{pmatrix} 1 & z^{2^k} \\ 1 & -z^{2^k} \end{pmatrix} \begin{pmatrix} 1 & z^{2^{k-1}} \\ 1 & -z^{2^{k-1}} \end{pmatrix} \cdots \begin{pmatrix} 1 & z \\ 1 & -z \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Let

$$g(z) := \frac{1}{\sqrt{2}} \begin{pmatrix} iz^{-1} & iz \\ iz^{-1} & -iz \end{pmatrix},$$

which is an element of $SU(2)$ for $|z| = 1$ and may be seen as a normalized version of the matrices above. Indeed,

$$\begin{pmatrix} (iz/\sqrt{2})^{k+1} P_k(z^2) \\ (iz/\sqrt{2})^{k+1} Q_k(z^2) \end{pmatrix} = g(z^{2^k}) \cdots g(z) \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{1}$$

We will prove a conjecture of Saffari:

Theorem 1 (Saffari's Conjecture)**.** *For ω a random variable distributed uniformly on the unit circle, $|\omega| = 1$,*

$$\mathbb{E}\Big| \frac{P_k(\omega)}{\sqrt{2^{k+1}}} \Big|^{2n} \sim \frac{1}{n+1}$$

as $n \to \infty$.

This characterizes the radial distribution of $P_k(\omega)/\sqrt{2^{k+1}}$. Likely this normalized polynomial is uniformly distributed in the unit circle (the conjecture of Montgomery), but we don't prove this here.

Noting that $P_k(\omega)$ has the same distribution as $P_k(\omega^2)$, Theorem 1 will be a consequence of

Theorem 2 (Equidistribution)**.** *For ω a random variable uniformly distributed on the unit circle, the matrix product*

$$g(\omega^{2^k})\cdots g(\omega)$$

tends in distribution to Haar measure on $SU(2)$.

The conjecture of Saffari then follows by examining the distribution of $g\begin{pmatrix}1\\0\end{pmatrix}$ for $g \in SU(2)$ distributed according to Haar measure. (One may use Euler angles for instance.)

The moral of Theorem 2 is clear; it is that $\omega, \omega^2, ..., \omega^{2^k}$ resemble i.i.d random variables $\omega_0, ..., \omega_k$ so that the matrix product in the theorem resembles a random walk (which may be seen to be supported on no proper subgroup of $SU(2)$ and to be aperiodic). We shall not prove the theorem using this method however – instead we take a step backwards and make use of the representation theory of $SU(2)$.

Indeed, if we can show for every nontrivial irreducible representation π of $SU(2)$ that

$$\mathbb{E}\,\pi(g(\omega^{2^k})\cdots g(\omega) = \mathbb{E}\,\pi(g(\omega^{2^k}))\cdots\pi(g(\omega)) \to 0,$$

then we will have demonstrated the theorem. This is really just a variant of the moment method in this context, and fortunately the representation theory of $SU(2)$ is elegant and well understood (see, e.g., Vilenkin's monograph).

Any matrix of $SU(2)$ has the form

$$g = \begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix},$$

with $|\alpha|^2 + |\beta|^2 = 1$. Nontrivial irreducible representations are parameterized by half-integers $\ell = 1/2, 1, 3/2, ...$ and consist of the matrices with entries

$$t^{\ell}_{mn} = \sqrt{\frac{(\ell-m)!(\ell+m)!}{(\ell-n)!(\ell+n)!}}\int_{\Gamma}(\alpha z+\gamma)^{\ell-n}(\beta z+\delta)^{\ell+n}z^{m-\ell}\frac{dz}{2\pi i z},$$

where $m, n \in \{-\ell, -(\ell-1), ..., \ell\}$, and the contour Γ is the unit circle. Note that

$$t^{\ell}_{m,n}(g(\omega)) = \underbrace{\sqrt{\frac{(\ell-m)!(\ell+m)!}{(\ell-n)!(\ell+n)!}}\frac{(-1)^{\ell}}{2^{\ell}}\int_{\Gamma}(z+1)^{\ell-n}(z-1)^{\ell+n}z^{m-\ell}\frac{dz}{2\pi i z}}_{\tilde{t}^{\ell}_{mn}}\,\omega^{2n},$$

with $\tilde{t}^{\ell}_{mn}$ itself a unitary matrix, corresponding to the representation of the matrix $g(1)$.

If $\ell = 1/2, 3/2, 5/2, ...$ then it is transparent that

$$\mathbb{E}\,t^{\ell}(g(\omega^{2^k}))\cdots t^{\ell}(g(\omega)) = 0,$$

for all $n \geq 0$, since every entry of the matrix product of which we are taking the expectation will be a polynomial in ω and ω^{-1} with only odd powers.

On the other hand, for $\ell = 1, 2, ...$ nothing so simple is true. Each entry of $t^\ell(g(\omega^{2^k})) \cdots t^\ell(g(\omega))$ will be a polynomial in ω and ω^{-1} with even exponents however, so at least we have

$$\mathbb{E}\, t^\ell(g(\omega^{2^k})) \cdots t^\ell(g(\omega)) = \mathbb{E} t^\ell(g(\omega^{2^{k-1}})) \cdots t^\ell(g(\omega^{-1/2}))$$

We use the notation:

$$T^\ell(\omega) := \tilde{t}^\ell \begin{pmatrix} \omega^{-\ell} & & & \\ & \omega^{-(\ell-1)} & & \\ & & \ddots & \\ & & & \omega^\ell \end{pmatrix} = t^\ell(g(\omega^{1/2})).$$

In order to show $\mathbb{E} T^\ell(\omega^{2^k}) \cdots T^\ell(\omega) \to 0$ as we must to prove the theorem, we need only show that all constant coefficients in $T^\ell(\omega^{2^k}) \cdots T^\ell(\omega)$ go to 0. To this end we note that following two facts:

i. The matrix entries of $T^\ell(\omega^{2^k}) \cdots T^\ell(\omega)$ will be polynomials in ω and ω^{-1}, lying in the span of $\{\omega^{(2^{k+1}-1)\ell}, ..., \omega^{-(2^{k+1}-1)\ell}\}$.

ii. The coefficients of $\omega^{\nu 2^{k+1}}$ for $\nu \in \mathbb{Z}$ (and in particular constant coefficients) of $T^\ell(\omega^{2^k}) \cdots T^\ell(\omega)$ are determined entirely by the coefficients of $\omega^{\nu 2^k}$ for $\nu \in \mathbb{Z}$ of $T^\ell(\omega^{2^{k-1}}) \cdots T^\ell(\omega)$.

We let P be the space of Laurent polynomials in ω (with complex coefficients) and define an operator S^ℓ on the product space $P^{2\ell+1}$ as follows: if for $A \in P^{2\ell+1}$,

$$T^\ell(\omega)A = T^\ell(\omega) \begin{bmatrix} A_{-\ell}(\omega) & \cdots & A_\ell(\omega) \end{bmatrix}^T = \begin{bmatrix} \sum_{j\in\mathbb{Z}} \beta_{-\ell}(j)\omega^j & \cdots & \sum_{j\in\mathbb{Z}} \beta_\ell(j)\omega^j \end{bmatrix}^T,$$

we define

$$S^\ell A := \begin{bmatrix} \sum_{j\in\mathbb{Z}} \beta_{-\ell}(2j)\omega^j & \cdots & \sum_{j\in\mathbb{Z}} \beta_\ell(2j)\omega^j \end{bmatrix}^T$$

For any $v \in \mathbb{C}^{2\ell+1}$, note that

$$\mathbb{E}\, T^\ell(\omega^{2^k}) \cdots T^\ell(\omega) v = \mathbb{E}\, (S^\ell)^{k+1} v.$$

Moreover, note that if $P_\ell = \mathrm{span}_\mathbb{C}\{\omega^{-(\ell-1)}, ..., \omega^{\ell-1}\}$, then S^ℓ maps $(P_\ell)^{2\ell+1}$ into itself. We let S_ℓ be the operator S^ℓ restricted to $(P_\ell)^{2\ell+1}$. If we show the spectral radius of S_ℓ is strictly less than 1, by a standard argument, we will have therefore proved the theorem. The remainder of the note is devoted to a proof of this fact.

Let $\rho(\cdot)$ denote the spectral radius of an operator. We note that

i. Because $T^\ell(\omega)$ is unitary and S^ℓ is just a subsequent projection onto even polynomials, we have $\rho(S^\ell) \leq 1$, and therefore, since S_ℓ is just a restriction of this operator, we have $\rho(S_\ell) \leq 1$ as well.

ii. If S_ℓ has an eigenvalue c with $|c| = 1$, then there must exist non-zero $A \in (P_\ell)^{2\ell+1}$ such that

$$T^\ell(\omega)A(\omega) = cA(\omega^2).$$

The reason is as follows. From the definition if S_ℓ has an eigenvalue with modulus 1, there must exist non-zero $A \in (P_\ell)^{2\ell+1}$ and a polynomial vector B of dimension $2\ell + 1$ with

$$T^\ell(\omega)A(\omega) = cA(\omega^2) + \omega B(\omega^2),$$

by dividing the polynomial vector on the left hand side into odd and even powers. But because $T^\ell(\omega)$ is unitary and A and B have complementary powers, this implies

$$\mathbb{E}\,\|A(\omega)\|_{\ell^2}^2 = |c| \cdot \mathbb{E}\,\|A(\omega^2)\|_{\ell^2}^2 + \mathbb{E}\,\|B(\omega^2)\|_{\ell^2}^2 = |c| \cdot \mathbb{E}\,\|A(\omega)\|_{\ell^2}^2 + \mathbb{E}\,\|B(\omega)\|_{\ell^2}^2$$

but since $|c| = 1$ by hypothesis, this implies $B = 0$.

We therefore will be done if we can show that the only $A \in (P_\ell)^{2\ell+1}$ satisfying $T^\ell(\omega)A(\omega) = cA(\omega^2)$ is $A = 0$. Labelling the coefficients of A, we are looking to find numbers $\alpha_h(j)$ such that

$$\tilde{t}^\ell \begin{pmatrix} \omega^{-\ell} & & & \\ & \omega^{-(\ell-1)} & & \\ & & \ddots & \\ & & & \omega^\ell \end{pmatrix} \begin{pmatrix} \sum_{j=-(\ell-1)}^{\ell-1} \alpha_{-\ell}(j)\omega^j \\ \vdots \\ \sum_{j=-(\ell-1)}^{\ell-1} \alpha_\ell(j)\omega^j \end{pmatrix} = c \begin{pmatrix} \sum_{j=-(\ell-1)}^{\ell-1} \alpha_{-\ell}(j)\omega^{2j} \\ \vdots \\ \sum_{j=-(\ell-1)}^{\ell-1} \alpha_\ell(j)\omega^{2j} \end{pmatrix}$$

By coupling coefficients this gives us a system of linear equations. We outline the proof that the only solution of this system of equations is $\alpha_h(j) = 0$ for all h, j, the demonstration of which completes the proof Theorem 1. (Written out more properly, the argument takes a few pages, with some kind of ugly notational issues that I hope to make better with more thought.)

Let $\mathcal{L}(\nu)$ be the linear equation in the coefficients $\alpha_h(j)$ that results from examining the coefficient of ω^ν above. Meaningful information is got from $\mathcal{L}(\nu)$ for $-2\ell + 1 \le \nu \le 2\ell - 1$. The information we need about $\tilde{t}^\ell$ in solving this system is not very special; we need

i. $\tilde{t}^\ell$ is invertible.

ii. $|\tilde{t}^\ell_{00}| < 1$.

iii. $\tilde{t}^\ell$ satisfies the following property: if any of the following hold,

$$\tilde{t}^\ell \begin{pmatrix} \beta_{-\ell} \\ \vdots \\ \beta{-1} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \gamma_0 \\ 0 \\ \gamma_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{or} \quad \tilde{t}^\ell \begin{pmatrix} \beta_{-\ell} \\ \vdots \\ \beta{-1} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \gamma_0 \\ 0 \\ \gamma_1 \\ 0 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{pmatrix} \quad \text{or} \quad \tilde{t}^\ell \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \beta_1 \\ \vdots \\ \beta_\ell \end{pmatrix} = \begin{pmatrix} 0 \\ \gamma_0 \\ 0 \\ \gamma_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ \beta_1 \\ \vdots \\ \beta_\ell \end{pmatrix} = \begin{pmatrix} \gamma_0 \\ 0 \\ \gamma_1 \\ 0 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{pmatrix},$$

then $\beta_i = 0$ and $\gamma_i = 0$ for all i.

The claim iii. is the only non-trivial statement here; it follows from using the explicit calculation of $\tilde{t}^\ell$ to show that any of these statements implies a polynomial identity that is impossible unless $\beta_i, \gamma_i = 0$ for all i.

Using these claims, we examine first the linear equations $\mathcal{L}(-2\ell+1), \mathcal{L}(-2\ell+3), ..., \mathcal{L}(2\ell-1)$. Using i. one can see straightforwardly in this way that the matrix $[\alpha_h(j)]$ (with j constant in columns, and h constant in rows) has 0 entries along alternating skew diagonals. We now consider $\mathcal{L}(-2(\ell-1))$ and see from iii. that the first column of $\alpha_h(j)$ has all 0 entries. We now iteratively consider $\mathcal{L}(-2(\ell-2))$, $\mathcal{L}(-2(\ell-3))$, ..., $\mathcal{L}(-2)$ to see again from iii. that each of the first $\ell-1$ columns of $[\alpha_h(j)]$ are 0 (being careful to update our information about which entries of the matrix are 0 with each step of the iteration) and also that the first $2\ell-1$ skew-diagonals of the matrix are 0. Proceeding in the opposite direction, we iteratively consider $\mathcal{L}(2(\ell-1), \mathcal{L}(2(\ell-2), ..., \mathcal{L}(2)$ to see in the same fashion as before that the last $\ell-1$ rows of $[\alpha_h(j)]$ are 0 and the last $2\ell-1$ skew-diagonals are 0. This process leaves only one entry $\alpha_0(0)$ that could be non-zero, but we can show $\alpha_0(0) = 0$ as well by using property ii.

This argument thus shows that all eigenvalues of S_ℓ must have modulus less than 1 and therefore proves Theorem 2 and Saffari's Conjecture, at least if I have made no mistake.

Best,
Brad Rodgers