The Degree 8 Examples in Davenport's Problem

Peter Müller

November 30, 2006

Abstract

Davenport conjectured[1] that a polynomial $f(X) \in \mathbb{Q}[X]$ is, up to a linear substitution over $\mathbb{Q}$, uniquely given by its value sets modulo all but finitely many primes. We classify the degree 8 counter-examples, and conjecture that all counter-examples are derived from these degree 8 examples.

1 Introduction

Let $f \in \mathbb{Q}[X]$ be a polynomial. If the prime p does not divide any denominator of f, then the value set $f(\mathbb{F}_p)$ on the field with p elements is defined. Two polynomials $f, g \in \mathbb{Q}[X]$ are said to be *Kronecker conjugate*, if $f(\mathbb{F}_p) = g(\mathbb{F}_p)$ holds for all but finitely many primes p. This happens of course if f and g differ by a linear substitution over $\mathbb{Q}$, that is, $f(X) = g(aX + b)$ with $0 \neq a \in \mathbb{Q}$, $b \in \mathbb{Q}$. In this case we say that f and g are *linearly related over* $\mathbb{Q}$. A Kronecker conjugate pair which is not linearly related over $\mathbb{Q}$ is called *properly Kronecker conjugate*. See [FJ05, Chapter 21.6] or [Mül98] for a more thorough introduction to this question and basic results.

Pairs of Kronecker conjugate polynomials have the same degrees (see below). The first serious progress in Davenport's problem was Fried's result that there are no pairs (f, g) of properly Kronecker conjugate polynomials if f is functionally indecomposable in $\mathbb{Q}[X]$. This follows from [Fri74, Section 2] combined with [Fri73, Section 3]. In [Mül98] this was extended to the case

[1] Orally communicated to M. Fried in 1968

that f has composition length 2, again there are no properly Kronecker conjugate examples. Thus potential counter-examples have composition length 3, in particular they need to have degree at least 8. The pair $(X^8, 16X^8)$ is an almost trivial counter-example. A closer look shows that there is actually a 1-parameter family of counter-examples of degree 8. We classify them all. In particular, the open problem 21.6.2 in [FJ05] need to be modified. Note that $d = 0$ below gives the known examples $f = X^8$, $g = 16X^8$. The polynomial f given below fulfills $f(Z - d/Z) = Z^8 + (d/Z)^8 - 2d^4$, so $f(X) = D_8(X, -d)$, where $D_n(X, a)$ denotes the Dickson polynomial of the first kind of degree 8.

Theorem. *For $d \in \mathbb{Q}$ set $f(X) = ((X^2+2d)^2-2d^2)^2$ and $g(X) = f(\sqrt{2}X) = ((2X^2 + 2d)^2 - 2d^2)^2$. Then f and g are properly Kronecker conjugate. Conversely, if F and G is a pair of properly Kronecker polynomials of degree 8, then there are $a, b \in \mathbb{Q}$ such that F is linearly related to $af + b$, and G is linearly related to $ag + b$.*

I believe that all examples are derived from f and g. Using the computer algebra system Magma I have verified it up to degree 30. (This was also done in the diploma thesis by Lu Dan.)

Conjecture. *Let $F, G \in \mathbb{Q}[X]$ be a pair of properly Kronecker conjugate polynomials. Then there is a polynomial $h(X) \in \mathbb{Q}[X]$, such that F and G are linearly related to $h(f(X))$ and $h(g(X))$, respectively, with f and g as in the Theorem.*

2 Grouptheoretic reformulation

Let $f, g \in \mathbb{Q}[X]$ be two non-constant polynomials, and t a transcendental over $\mathbb{C}$. Let L be a common splitting field of $f(X) - t$ and $g(X) - t$ over $\mathbb{Q}(t)$. The main tool for studying Davenport's problem is

Proposition 2.1 (Fried)**.** *The following are equivalent.*

(a) f and g are Kronecker conjugate.

(b) Each element of $\mathrm{Gal}(L/\mathbb{Q}(t))$ fixes a root of $f(X) - t$ if and only if it fixes a root of $g(X) - t$.

Fried's original proof used Cebotarev's density theorem for function fields over finite fields. A modification, which also uses model theory, can be found in [FJ05]. Another proof, based on Hilbert's irreducibility theorem and Frobenius' density theorem for number fields, is given in [Mül98].

If two polynomials are Kronecker conjugate, then they have the same degree, see [FJ05, 21.6.7]. Furthermore, $\mathrm{Gal}(L/\mathbb{Q}(t))$ acts faithfully on the roots of $f(X)-t$ as well as on the roots of $g(X)-t$. Thus consider $A = \mathrm{Gal}(L/\mathbb{Q}(t))$ as a faithful permutation group on the n roots of $f(X)-t$. Let V be a stabilizer in A of a root of $g(X)-t$. Then, by the above proposition, f and g are Kronecker conjugate if and only if the union $\bigcup_{a\in A} V^a$ of the conjugates of V consists precisely of those elements of A which fix at least one fixed. Suppose f and g are properly Kronecker conjugate. As f and g have the same degree, we get $[A:V] = n$. Thus if V would fix a point, then it would be the stabilizer in A of this point. Thus some root of $f(X)-t$ is contained in the field generated by $\mathbb{Q}$ and a root of $g(X)-t$. This easily shows that f and g are linearly related over $\mathbb{Q}$. Therefore V does not fix a point.

Let $G = \mathrm{Gal}(L\mathbb{C}/\mathbb{C}(t))$. Clearly, G is a normal subgroup of A. As $f(X)-t$ is irreducible over $\mathbb{C}(t)$, we get that G is still transitive on G. However, more is true: It is well known (see e.g. [Mül98]) that G is the monodromy group of the branched covering $\mathbb{P}^1 \to \mathbb{P}^1$, $z \mapsto f(z)$ of Riemann spheres. The action of G on the roots of $f(X)-t$ is equivalent to the action of G on a regular fiber of the covering. From that one obtains (see [Mül98]) that G is generated by elements $\sigma_1, \sigma_2, \ldots, \sigma_r$ such that the product $\sigma_1\sigma_2\ldots\sigma_r$ is an n-cycle, and $\sum_{i=1}^{r} \operatorname{ind}\sigma_i = n-1$, where $\operatorname{ind}\sigma$ denotes n minus the number of cycles of σ.

Let $\mathrm{AGL}_1(8)$ be the group of permutations $x \mapsto ax+b$ on $\mathbb{Z}/8\mathbb{Z}$ for all $a \in (\mathbb{Z}/8\mathbb{Z})^\star$, $b \in \mathbb{Z}/8\mathbb{Z}$.

Proposition 2.2. *Let f and g be a Kronecker conjugate pair of polynomials of degree 8. Then after suitably identifying the roots of $f(X)-t$ with the elements in $\mathbb{Z}/8\mathbb{Z}$, we have $A = \mathrm{AGL}_1(8)$ and all orbits of V have length 2. Furthermore, either G is cyclic of order 8, or $r = 2$ and $\sigma_1 = (x \mapsto ax)$, $\sigma_2 = (x \mapsto ax+1)$ with $a \in \{-1, 3\}$. In any case, $G \cap V$ is a point-stabilizer in G.*

Proof. By Fried's branch cycle argument (confer e.g. [Mül98, Section 2.2]), we know that $\mathrm{AGL}_1(8) \leq A$. On the other hand, f is a composition of 3 polynomials of degree 2 by [Mül98, Theorem 1.2]. Thus A has a chain of

subgroups $A > M > K > U$ descending by index 2, and U is a point-stabilizer (see [Mül98, 2.7]). Thus A is a 2-group. As V is a 2-group, and each element of V fixes at least 2 points, we obtain that V has at least 3 orbits. As V does not fix a point, the orbit lengths are $2, 2, 2, 2$ or $2, 2, 4$. The orbit lengths of a point-stabilizer of $\mathrm{AGL}_1(8)$ are $1, 1, 2, 4$. As U contains this point-stabilizer and fixes a point, we obtain that U has the same orbit lengths $1, 1, 2, 4$. Thus $U <\leq C_2 \times D_4$. Here C_n denotes the cyclic group of order n in its regular action, and D_n the degree n action of the dihedral group of order $2n$. Hence $|U| \leq 16$.

We claim that $|U| \leq 8$. Suppose that $U = C_2 \times D_4$. By Kronecker conjugacy V contains a 4-cycle, and a product of a 4 cycle with disjoint transposition. From the orbit structure of V we obtain $1 \times C_2 \times C_4 \leq V$ (with the first factor acting trivially on 2 points). As V does not fix point, there is an element $(\alpha, \beta, \gamma) \in V$ with a transposition α. We may assume $\alpha = \beta$, so $(\alpha, \alpha, \gamma\delta) \in V$ for each $\delta \in C_4$. However, D_4 contains only three elements with fixed points, so the coset γC_4 contains a fixed point free element, giving a fixed point free element in V, a contradiction.

Thus $|U| \leq 8$, so $[A : \mathrm{AGL}_1(8)] \leq 2$. The derived subgroup of $\mathrm{AGL}_1(8)$ is generated by $\tau = (1, 3, 5, 7)(2, 4, 6, 8)$. We obtain that A normalizes $<\tau>$. Suppose that $|U| = 8$ and that U fixes 1. Then U is generated by $(2, 4, 6, 8)$ and $(3, 7)(4, 6)$. In particular, U contains a 4-cycle, and so does V. Thus V has orbit lengths $2, 2, 4$, and V contains at least 2 nontrivial elements with at least 4 fixed points. Thus the number of orbits of V is at least $\frac{1}{8}(8 + 2 \cdot 4 + 5 \cdot 2) > 3$, a contradiction.

Thus $A = \mathrm{AGL}_1(8)$, so $|V| = 4$. Each element in V has at least 2 fixed points, so V has at least $\frac{1}{4}(8 + 3 \cdot 2) = \frac{7}{2} > 3$ orbits. On the other hand, each orbit of V has length ≥ 2, and the claim follows. It remains to compute the generating system $\sigma_1, \ldots, \sigma_r$ for G. If $r = 1$ then σ_1 is an 8-cycle, and $G = C_8$. Thus suppose $r \geq 2$. The sum of the $\operatorname{ind} \sigma_i$ is 7, and clearly $\operatorname{ind} \sigma \geq 2$ for all $1 \neq \sigma \in A$, so $r \leq 3$. Let C be generated by $x \mapsto x + 1$. If $r = 3$, then without loss of generality $(\operatorname{ind} \sigma_1, \operatorname{ind} \sigma_2, \operatorname{ind} \sigma_3) = (2, 2, 3)$. But $\operatorname{ind} \sigma = 2$ if and only if $\sigma = (x \mapsto 5x + \epsilon)$ with $\epsilon \in \{0, 4\}$. So $\sigma_1\sigma_2 \in C$, hence $\sigma_3 \in C$, a contradiction.

Thus $r = 2$ and $(\operatorname{ind} \sigma_1, \operatorname{ind} \sigma_2) = (3, 4)$. By conjugation with an element from C we may assume that σ_1 fixes 0, so $\sigma_1 = (x \mapsto ax)$ with $a \in (\mathbb{Z}/8\mathbb{Z})^\star$. But $\operatorname{ind} \sigma_1 = 3$ forces $a = -1$ or $a = 3$. We get $\sigma_2 = \sigma_1^{-1}(x \mapsto x + 1) = (x \mapsto ax + 1)$. □

3 Computation of the pairs (f, g)

We start to compute f. From the structure of A it is clear that f is a composition of 3 quadratic polynomials. A branch point of f is a number $c \in \mathbb{C}$ such that the fiber $f^{-1}(c)$ consists of less than 8 elements. Suppose that $r = 2$ and that σ_1 and σ_2 are as in the proposition above. Then f has two branch points b_1 and b_2. The multiplicities of the roots of $f(X) - b_i$ are the cycle lengths of σ_i. If $b_i \neq \mathbb{Q}$, then there is an automorphism σ of $\mathbb{C}$ with $b_i^\sigma \neq b_i$. But then b_i^σ is another branch point, and the corresponding σ has the same cycle lengths. However, σ_1 and σ_2 have 3 and 4 cycles (of length 2) respectively, so $b_i \in \mathbb{Q}$. By linear changes over $\mathbb{Q}$ we may assume that $b_2 = 0$, f is monic, and the penultimate coefficient of f vanishes. Furthermore the cycle type of σ_2 tells us that $f(X)$ is the square of a separable polynomial, so $f(X) = (X^4 + aX^2 + bX + c)^2$ with $a, b, c \in \mathbb{Q}$. As $X^4 + aX^2 + bX + c$ is the composition of two quadratic polynomials, we may assume $X^4 + aX^2 + bX + c = (X^2 + 2d)^2 + e$, so

$$f(X) = ((X^2 + 2d)^2 + e)^2 \text{ with } d, e \in \mathbb{Q} \setminus \{0\}.$$

Clearly e^2 is a branch point of $f(X)$, so this must correspond to σ_1. Thus the multiplicities of the roots of $f(X) - e^2$ are $1, 1, 2, 2, 2$. As

$$f(X) - e^2 = (X^2 + 2d)^2(X^4 + 4dX^2 + 4d^2 + 2e)$$

we obtain that $X^4 + 4dX^2 + 4d^2 + 2e$ has two simple roots and one multiple root. The discriminant of $X^4 + 4dX^2 + 4d^2 + 2e$ is (up to a constant factor) $(2d^2 + e)e^2$, thus $e = -2d^2$. We obtain

$$f(X) = ((X^2 + 2d)^2 - 2d^2)^2.$$

If we allow $d = 0$, then $f(X) = X^8$. This case corresponds to the possibility $G = C_8$. Therefore, allowing $d = 0$, we cover all possible cases from the proposition. It remains to find g. By a linear change over $\mathbb{Q}$ of the argument of g we may assume that the penultimate coefficient of g vanishes. As $V \cap G$ has order at most 2, we see that $V \cap G$ fixes a root of $f(X) - t$. Thus f and g are linearly related over $\mathbb{C}$. As the penultimate coefficients of f and g both vanish, we get $\lambda \in \mathbb{C}$ with $g(X) = f(\lambda X)$. From

$$g(X) = f(\lambda X) = \lambda^8 X^8 + 8\lambda^6 dX^6 + \cdots \in \mathbb{Q}[X]$$

we obtain $\lambda^2 \in \mathbb{Q}$, provided that $d \neq 0$. For the moment assume $d \neq 0$. All orbits of V have length 2, so the irreducible factors of $f(X) - g(Y)$ over $\mathbb{Q}(Y)$ have degree 2. We have

$$\begin{aligned} f(X) - g(Y) &= f(X) - f(\lambda Y) \\ &= ((X^2 + 2d)^2 - ((\lambda Y)^2 + 2d)^2) \\ &\quad ((X^2 + 2d)^2 + ((\lambda Y)^2 + 2d)^2 - 4d^2) \\ &= (X^2 - \lambda^2 Y^2)(X^2 + \lambda^2 Y^2 + 4d) \\ &\quad (X^4 + 4dX^2 + \lambda^4 Y^4 + \lambda^2 dY^2 + 4d^2). \end{aligned}$$

Write $\ell = \lambda^2 \in \mathbb{Q} \setminus \{0\}$. So $X^4 + 4dX^2 + \ell^2 Y^4 + 4\ell dY^2 + 4d^2$ is a product of two polynomials of degree 2 in X. Therefore there are $U, V, W \in \mathbb{Q}[Y]$ with

$$X^4 + 4dX^2 + \ell^2 Y^4 + 4\ell dY^2 + 4d^2 = (X^2 + UX + V)(X^2 - UX + W).$$

Comparing coefficients yields

$$\begin{aligned} V + W - U^2 &= 4d \\ U(V - W) &= 0 \\ VW &= \ell^2 Y^4 + 4\ell dY^2 + 4d^2. \end{aligned}$$

Suppose first that $U = 0$. Then $V + W = 4d$ and $VW = \ell^2 Y^4 + 4\ell dY^2 + 4d^2$. This gives

$$(V - 2d)^2 = -\lambda Y^4 - 4\lambda dY^2 = -4\lambda Y^2(\lambda Y^2 + 4d).$$

But $\lambda Y^2 + 4d$ is separable, hence not a square in $\mathbb{C}[Y]$. Therefore $U \neq 0$, so $V = W$. Thus

$$V^2 = \ell^2 Y^4 + 4\ell dY^2 + 4d^2 = (\ell Y^2 + 2d)^2.$$

Again, $\ell Y^2 + 2d$ is separable, so $V = W = \pm(\ell Y^2 + 2d)$. This gives

$$U^2 = V + W - 4d = \pm 2(\ell Y^2 + 2d) - 4d.$$

As $-2(\ell Y^2 + 2d) - 4d$ is separable, we must have the other case

$$U^2 = 2(\ell Y^2 + 2d) - 4d = 2\ell Y^2.$$

Thus 2ℓ is a square, so up to linear changes over $\mathbb{Q}$ of g we may assume $\lambda = \sqrt{2}$.

We get the same conclusion in the case $f = X^8$, $g = \lambda^8 X^8$ as follows. Again, $X^8 - \lambda^8 Y^8$ is a product of irreducible factors over $\mathbb{Q}(Y)$ of degree 2. In particular, there is $\mu \neq 1$ with $\mu^8 = 1$ and $(X - \lambda Y)(X - \lambda\mu Y) \in \mathbb{Q}[X, Y]$, hence

$$\begin{aligned} \lambda(\mu + 1) &\in \mathbb{Q} \\ \lambda^2 \mu &\in \mathbb{Q}. \end{aligned}$$

From that we get $\mu + \frac{1}{\mu} = \frac{(\lambda(\mu+1))^2}{\lambda^2 \mu} \in \mathbb{Q}$. First suppose $\mu \neq -1$. Then the minimal polynomial of μ has degree at least 2. On the other hand, there is $a \in \mathbb{Q}$ with $\mu^2 - a\mu + 1 = 0$. The only irreducible degree 2 factor of $X^8 - 1$ is $X^2 + 1$, so $a = 0$, hence $\mu^2 = -1$. Let $\lambda(\mu + 1) = b \in \mathbb{Q}$. Then

$$\lambda^2 = \frac{b^2}{(\mu + 1)^2} = \frac{b^2}{2\mu}.$$

Now $\mu^4 = 1$, no matter if $\mu = -1$ or $\mu^2 = -1$. So we obtain

$$\lambda^8 = (\frac{b^2}{2\mu})^4 = \frac{b^8}{16}.$$

This shows that, up to a linear change over $\mathbb{Q}$, that g has the form $g(X) = 16X^8 = (\sqrt{2}X)^8$.

We are left to show that the pairs f, g we constructed are indeed properly Kronecker conjugate. They are obviously not linearly related over $\mathbb{Q}$, so we just need to verify Kronecker conjugacy. A somewhat cumbersome approach would be to compute Galois groups and apply Fried's proposition. Instead, we prefer to directly verify the arithmetic property. Setting $\lambda = \sqrt{2}$ we compute

$$\begin{aligned} f(X) - g(Y) &= (X^2 - 2Y^2)(X^2 + 2Y^2 + 4d)(X^2 - 2XY + 2Y^2 + 2d) \\ &\quad (X^2 + 2XY + 2Y^2 + 2d) \\ &= (X^2 - 2Y^2)(X^2 + 2(Y^2 + 2d))((X - Y)^2 + (Y^2 + 2d)) \\ &\quad ((X + Y)^2 + (Y^2 + 2d)). \end{aligned}$$

Let p be a prime which does not divide the denominator of d. We claim that $g(\mathbb{F}_p) \subseteq f(\mathbb{F}_p)$. For this choose $y \in \mathbb{F}_p$, and suppose that there is no $x \in \mathbb{F}_p$ with $f(x) = g(y)$. Then the first three factors of the above factorization show that 2, $-2(y^2 + 2d)$ and $-(y^2 + 2d)$ are non-squares in $\mathbb{F}_p$. However,

the product of these three elements is a square in $\mathbb{F}_p$, so one of the factors is a square, a contradiction.

The other inclusion $f(\mathbb{F}_p) \subseteq g(\mathbb{F}_p)$ follows analogously for odd primes p not dividing the denominator of d.

References

[FJ05] M. D. Fried, M. Jarden, *Field Arithmetic*, vol. 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*, Springer-Verlag, Berlin, 2nd edn. (2005).

[Fri73] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. (1973), **17**, 128–146.

[Fri74] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory (1974), **6**, 211–231.

[Mül98] P. Müller, *Kronecker conjugacy of polynomials*, Trans. Amer. Math. Soc. (1998), **350**, 1823–1850.

Institut für Mathematik, Universität Würzburg, Am Hubland, 97074 Würzburg, Germany
E-mail: Peter.Mueller@mathematik.uni-wuerzburg.de